

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6909863号

(P6909863)

(45) 発行日 令和3年7月28日 (2021.7.28)

(24) 登録日 令和3年7月7日 (2021.7.7)

(51) Int. Cl. F I

HO 4W 76/14	(2018.01)	HO 4W 76/14
HO 4W 12/02	(2009.01)	HO 4W 12/02
HO 4W 12/06	(2021.01)	HO 4W 12/06
HO 4W 84/18	(2009.01)	HO 4W 84/18
HO 4W 76/12	(2018.01)	HO 4W 76/12

請求項の数 20 (全 62 頁) 最終頁に続く

(21) 出願番号 特願2019-548314 (P2019-548314)
 (86) (22) 出願日 平成30年2月28日 (2018.2.28)
 (65) 公表番号 特表2020-512732 (P2020-512732A)
 (43) 公表日 令和2年4月23日 (2020.4.23)
 (86) 国際出願番号 PCT/US2018/020121
 (87) 国際公開番号 WO2018/164901
 (87) 国際公開日 平成30年9月13日 (2018.9.13)
 審査請求日 令和1年10月23日 (2019.10.23)
 (31) 優先権主張番号 15/450,654
 (32) 優先日 平成29年3月6日 (2017.3.6)
 (33) 優先権主張国・地域又は機関
 米国 (US)

(73) 特許権者 397074301
 サイトリックス システムズ, インコーポ
 レイテッド
 アメリカ合衆国 フロリダ 33309,
 フォート ローダーデール, ウェスト
 サイプレス クリーク ロード 851
 110002310
 (74) 代理人 特許業務法人あい特許事務所
 (72) 発明者 ヴァリシェーラ, チャクラバルシ
 アメリカ合衆国, フロリダ州 33309
 , フォート ローダーデール, ウェスト
 サイプレス クリーク ロード 851,
 サイトリックス システムズ, インコーポ
 レイテッド内

最終頁に続く

(54) 【発明の名称】 ピアツーピア通信に基づく仮想プライベート・ネットワーキング

(57) 【特許請求の範囲】

【請求項 1】

メッシュ・ネットワークのメンバとして第1のモバイル・デバイスを構成することであ
 って、前記構成の後に、前記第1のモバイル・デバイスは、前記メッシュ・ネットワ
 ークを介したピアツーピア接続によって、第2のモバイル・デバイスと通信することが
 できる、前記構成することと、

前記第1のモバイル・デバイスから第2のモバイル・デバイスへ、前記メッシュ・ネッ
 トワークを介した前記ピアツーピア接続によって、シングル・サインオン (SSO) のた
 めに構成された有効な認証トークンであって、前記第2のモバイル・デバイスのセキュ
 ア・コンテナをロック解除し前記セキュア・コンテナへのSSOを可能にするために構成さ
 れた前記有効な認証トークンを送信することと、

前記第1のモバイル・デバイスによって、前記メッシュ・ネットワークを介した前記
 ピアツーピア接続によって、アクセス・ゲートウェイのための第1のデータを受信する
 ことであって、前記アクセス・ゲートウェイは、前記メッシュ・ネットワークとは異なる第
 2のネットワークを介して前記第1のモバイル・デバイスに接続されている、前記受信す
 ることと、

前記第1のモバイル・デバイスによって、前記第1のモバイル・デバイスと前記アクセ
 ス・ゲートウェイとの間の前記第2のネットワークを介した仮想プライベート・ネットワ
 ーク接続によって、前記第1のデータを前記アクセス・ゲートウェイに送信することと
 を含む方法。

10

20

【請求項 2】

前記第 1 のモバイル・デバイスによって、前記第 2 のネットワークを介した前記仮想プライベート・ネットワーク接続によって、前記第 2 のモバイル・デバイスのための第 2 のデータを受信することと、

前記仮想プライベート・ネットワーク接続に関連する暗号化解除鍵に基づいて前記第 2 のデータを暗号化解除し、その結果、暗号化解除された第 2 のデータをもたらすことと、

前記ピアツーピア接続に関連する暗号化鍵に基づいて前記暗号化解除された第 2 のデータを暗号化し、その結果、暗号化された第 2 のデータをもたらすことと、

前記第 1 のモバイル・デバイスによって、前記メッシュ・ネットワークを介した前記ピアツーピア接続によって、前記暗号化された第 2 のデータを前記第 2 のモバイル・デバイスに送信することと

10

をさらに含む、請求項 1 に記載の方法。

【請求項 3】

前記第 2 のデータは、前記第 2 のモバイル・デバイスのアプリケーション管理フレームワークによって実施されるポリシーに対する更新を含む、請求項 2 に記載の方法。

【請求項 4】

前記第 1 のデータは、前記有効な認証トークンを含み、

前記有効な認証トークンは、前記アクセス・ゲートウェイがシングル・サインオン（S S O）に基づいて前記第 2 のモバイル・デバイスを認証することを可能にする、請求項 1 に記載の方法。

20

【請求項 5】

前記第 2 のネットワークは、無線ネットワークであり、

前記第 1 のモバイル・デバイスによって前記無線ネットワークに接続することであって、前記仮想プライベート・ネットワーク接続は、前記無線ネットワークを通るトンネルとして構成され、前記第 2 のモバイル・デバイスは、前記無線ネットワークに接続されない、前記接続すること

をさらに含む、請求項 1 に記載の方法。

【請求項 6】

前記アクセス・ゲートウェイは、企業リソースへのアクセスを管理するように構成され、

30

前記メッシュ・ネットワークは、前記第 1 のモバイル・デバイス、前記第 2 のモバイル・デバイス、および第 3 のモバイル・デバイスを含み、

前記アクセス・ゲートウェイ用であり、かつ前記第 3 のモバイル・デバイスによって前記企業リソースにアクセスする要求を示す第 2 のデータを、前記第 1 のモバイル・デバイスが、前記メッシュ・ネットワークを介した前記ピアツーピア接続によって受信することと、

前記第 1 のモバイル・デバイスによって、前記第 2 のネットワークを介した前記仮想プライベート・ネットワーク接続によって、前記第 2 のデータを前記アクセス・ゲートウェイに送信することと、

前記第 1 のモバイル・デバイスによって、前記第 2 のネットワークを介した前記仮想プライベート・ネットワーク接続によって、前記企業リソースにアクセスする前記要求に基づく応答データを受信することと、

40

前記第 3 のモバイル・デバイスが前記応答データを受信するように、前記第 1 のモバイル・デバイスによって、前記応答データを、前記メッシュ・ネットワークを介してルーティングさせることと

をさらに含む、請求項 1 に記載の方法。

【請求項 7】

前記メッシュ・ネットワークは、前記第 1 のモバイル・デバイス、前記第 2 のモバイル・デバイス、および第 3 のモバイル・デバイスを含み、

前記第 1 のモバイル・デバイスによって、前記メッシュ・ネットワークを介した前記ピア

50

アツーパーピア接続によって、前記第3のモバイル・デバイスのための第2のデータを受信することと、

前記第3のモバイル・デバイスが前記第2のデータを暗号化された形で受信するように、前記第1のモバイル・デバイスによって、前記第2のデータを前記メッシュ・ネットワークを介してルーティングさせることと

をさらに含む、請求項1に記載の方法。

【請求項8】

前記ピアツーパーピア接続は、B L U E T O O T H（登録商標）接続またはW I - F I D I R E C T接続を含む、請求項1に記載の方法。

【請求項9】

前記第2のモバイル・デバイスによって、前記第1のモバイル・デバイスから前記メッシュ・ネットワークを介した前記ピアツーパーピア接続によって、前記有効な認証トークンを受信することと、

前記有効な認証トークンに基づいて、前記第2のモバイル・デバイスによって、前記セキュア・コンテナのための前記S S Oを使用可能にするために、前記セキュア・コンテナをロック解除することと、

をさらに含む、前記セキュア・コンテナは企業管理フレームワークに関連している、請求項1に記載の方法。

【請求項10】

1つまたは複数のプロセッサと、

前記1つまたは複数のプロセッサによって実行された時に、装置に下記の各工程を実行させる実行可能命令を記憶するメモリと、を含む前記装置。

- メッシュ・ネットワークのメンバとして前記装置を構成すること、ここにおいて、前記構成された後に、前記装置は、前記メッシュ・ネットワークを介したピアツーパーピア接続によって、第1のモバイル・デバイスと通信することができ、

- 前記第1のモバイル・デバイスへ、前記メッシュ・ネットワークを介した前記ピアツーパーピア接続によって、シングル・サインオン（S S O）のために構成された有効な認証トークンであって、前記第1のモバイル・デバイスのセキュア・コンテナをロック解除し前記セキュア・コンテナへのS S Oを可能にするために構成された前記有効な認証トークンを送信すること、

- 前記第1のモバイル・デバイスによって、前記メッシュ・ネットワークを介した前記ピアツーパーピア接続によって、アクセス・ゲートウェイのための第1のデータを受信することであって、前記アクセス・ゲートウェイは、前記メッシュ・ネットワークとは異なる第2のネットワークを介して前記装置に接続されている、前記受信すること、

- 前記第1のモバイル・デバイスによって、前記第1のモバイル・デバイスと前記アクセス・ゲートウェイとの間の前記第2のネットワークを介した仮想プライベート・ネットワーク接続によって、前記第1のデータを前記アクセス・ゲートウェイに送信すること。

【請求項11】

前記実行可能命令は、前記1つまたは複数のプロセッサによって実行された時に、前記装置に、

前記第2のネットワークを介した前記仮想プライベート・ネットワーク接続によって、前記第1のモバイル・デバイスのための第2のデータを受信させ、

前記仮想プライベート・ネットワーク接続に関連する暗号化解除鍵に基づいて前記第2のデータを暗号化解除させ、暗号化解除された第2のデータをもたらせ、

前記ピアツーパーピア接続に関連する暗号化鍵に基づいて前記暗号化解除された第2のデータを暗号化させ、暗号化された第2のデータをもたらせ、

前記メッシュ・ネットワークを介した前記ピアツーパーピア接続によって、前記第2のデータを前記第1のモバイル・デバイスに送信させる

請求項10に記載の装置。

【請求項12】

前記第2のデータは、前記第1のモバイル・デバイスのアプリケーション管理フレームワークによって実施されるポリシーに対する更新を含む、請求項11に記載の装置。

【請求項13】

前記第1のデータは、前記有効な認証トークンを含み、前記有効な認証トークンは、前記アクセス・ゲートウェイが前記SSOに基づいて前記第1のモバイル・デバイスを認証することを可能にする、請求項10に記載の装置。

【請求項14】

前記第2のネットワークは無線ネットワークを含み、

前記実行可能命令は、前記1つまたは複数のプロセッサによって実行された時に、前記装置に、

前記無線ネットワークに接続させ、前記仮想プライベート・ネットワーク接続は、前記無線ネットワークを通るトンネルとして構成され、前記第1のモバイル・デバイスは、前記無線ネットワークに接続されない

請求項10に記載の装置。

【請求項15】

前記アクセス・ゲートウェイは、企業リソースへのアクセスを管理するように構成され

前記実行可能命令は、前記1つまたは複数のプロセッサによって実行された時に、前記装置に、

前記メッシュ・ネットワークを介した前記ピアツーピア接続によって、前記アクセス・ゲートウェイ用の第2のデータであって、第2のモバイル・デバイスによって前記企業リソースにアクセスする要求を示す前記第2のデータを受信させ、前記メッシュ・ネットワークは、前記装置、前記第1のモバイル・デバイス、および前記第2のモバイル・デバイスを含み、

前記第2のネットワークを介した前記仮想プライベート・ネットワーク接続によって、前記第2のデータを前記アクセス・ゲートウェイに送信させ、

前記第2のネットワークを介した前記仮想プライベート・ネットワーク接続によって、前記企業リソースにアクセスする前記要求に基づく応答データを受信させ、

前記第2のモバイル・デバイスが前記応答データを受信するように、前記応答データを、前記メッシュ・ネットワークを介してルーティングさせる

請求項10に記載の装置。

【請求項16】

実行可能命令を記憶する1つまたは複数のコンピュータ可読媒体であって、前記実行可能命令が実行された時に、装置に下記の各工程を行わせるコンピュータ可読媒体。

- メッシュ・ネットワークのメンバとして前記装置を構成すること、ここにおいて、前記構成された後に、前記装置は、前記メッシュ・ネットワークを介したピアツーピア接続によって第1のモバイル・デバイスと通信することができ、

- 前記第1のモバイル・デバイスへ、前記メッシュ・ネットワークを介した前記ピアツーピア接続によって、シングル・サインオン（SSO）のために構成された有効な認証トークンであって、前記第1のモバイル・デバイスのセキュア・コンテナをロック解除し前記セキュア・コンテナへのSSOを可能にするために構成された前記有効な認証トークンを送信すること、

- 前記メッシュ・ネットワークを介した前記ピアツーピア接続によって、アクセス・ゲートウェイのための第1のデータを受信させ、ここにおいて、前記アクセス・ゲートウェイは、前記メッシュ・ネットワークとは異なる第2のネットワークを介して前記装置に接続されており、

- 前記装置と前記アクセス・ゲートウェイとの間の、前記第2のネットワークを介した仮想プライベート・ネットワーク接続によって、前記第1のデータを前記アクセス・ゲートウェイに送信する。

【請求項17】

10

20

30

40

50

前記実行可能命令は、実行された時に、前記装置に、
前記第2のネットワークを介した前記仮想プライベート・ネットワーク接続によって、
前記第1のモバイル・デバイス用である第2のデータを受信させ、
前記仮想プライベート・ネットワーク接続に関連する暗号化解除鍵に基づいて前記第2
のデータを暗号化解除し、その結果、暗号化解除された第2のデータをもたらせ、
前記ピアツーピア接続に関連する暗号化鍵に基づいて前記暗号化解除された第2のデー
タを暗号化し、その結果、暗号化された第2のデータをもたらせ、
前記メッシュ・ネットワークを介した前記ピアツーピア接続によって、前記暗号化され
た第2のデータを前記第1のモバイル・デバイスに送信させる
請求項16に記載の1つまたは複数のコンピュータ可読媒体。

10

【請求項18】

前記第2のデータは、前記第1のモバイル・デバイスのアプリケーション管理フレームワークによって実施されるポリシーに対する更新を含む、請求項17に記載の1つまたは複数のコンピュータ可読媒体。

【請求項19】

前記第2のネットワークは無線ネットワークを含み、
前記実行可能命令は、実行された時に、前記装置に、
前記無線ネットワークに接続させ、ここにおいて、前記仮想プライベート・ネットワー
ク接続は、前記無線ネットワークを通るトンネルとして構成され、前記第1のモバイル・
デバイスは、前記無線ネットワークに接続されない
請求項16に記載の1つまたは複数のコンピュータ可読媒体。

20

【請求項20】

前記アクセス・ゲートウェイは、企業リソースへのアクセスを管理するように構成され

、
前記実行可能命令は、実行された時に、前記装置に、
メッシュ・ネットワークを介した前記ピアツーピア接続によって、前記アクセス・ゲー
トウェイ用であり、かつ第2のモバイル・デバイスによる前記企業リソースにアクセスす
る要求を示す第2のデータを受信させ、前記メッシュ・ネットワークは、前記装置、前記
第1のモバイル・デバイス、および前記第2のモバイル・デバイスを含み、
前記第2のネットワークを介した前記仮想プライベート・ネットワーク接続によって、
前記第2のデータを前記アクセス・ゲートウェイに送信させ、
前記第2のネットワークを介した前記仮想プライベート・ネットワーク接続によって、
前記企業リソースにアクセスする前記要求に基づく応答データを受信させ、
前記第2のモバイル・デバイスが前記応答データを受信するように、前記応答データを、
前記メッシュ・ネットワークを介してルーティングさせる
請求項16に記載の1つまたは複数のコンピュータ可読媒体。

30

【発明の詳細な説明】

【技術分野】

【0001】

本明細書で説明される発明の諸態様は、全般的に、仮想プライベート・ネットワーキング、ピアツーピア通信、メッシュ・ネットワーキング、および／または企業モビリティ管理システムに関する。

40

【背景技術】

【0002】

今日のユーザは、しばしば、複数のコンピューティング・デバイスを使用する。たとえば、ユーザは、スマート・フォン、タブレット・コンピュータ、およびラップトップ・コンピュータを1日の異なる時刻に使用する場合がある。ユーザが、彼または彼女の日常生活により多数のデバイスを統合する時に、ユーザは、リモート位置から彼または彼女の雇用者（または何らかの他の企業）のリソースにアクセスし、使用するのにこれらのデバイスを使用することをますます望む可能性がある。これらのデバイスは、異なる能力を有す

50

る場合があり、リモート位置の動作環境に応じて、同一のネットワークに接続できない場合がある。たとえば、ユーザのスマート・フォンが、セルラ・ネットワークに接続されるが、ユーザのタブレットまたはラップトップ・コンピュータが、セルラ・ネットワークに接続できない場合がある。

【発明の概要】

【発明が解決しようとする課題】

【0003】

企業が、そのような動作環境内でスマート・フォンとラップトップとの両方からユーザが企業リソースにアクセスすることを可能にすることを望む場合に、企業は、複数の課題に直面する可能性がある。たとえば、セルラ・ネットワークが、ユーザの使用可能な唯一のネットワークである場合に、ユーザがタブレットまたはラップトップ・コンピュータから企業リソースにアクセスする能力を使用可能にすることが、課題である。さらに、ユーザが、タブレットまたはラップトップ・コンピュータから企業リソースにアクセスできる場合であっても、ユーザのアクセスが安全なままであることを保証することが、課題である。これらの課題に鑑みて、安全な形で複数のデバイスから企業リソースにアクセスするユーザの能力を改善する必要がある。

【課題を解決するための手段】

【0004】

以下では、本明細書で説明される発明の様々な態様の単純化された概要を提示する。この概要は、広範囲の概要ではなく、主要なもしくはクリティカルな要素を識別することまたは特許請求の範囲の範囲を詳細に描写することは意図されていない。以下の概要は、単に、下で提供されるより詳細な説明の導入の前置きとして単純化された形でいくつかの概念を提示するものである。

【0005】

上で説明した従来技術の制限を克服するため、および本明細書を読み、理解した時に明白になる他の制限を克服するために、本明細書で説明される諸態様は、たとえば、複数のモバイル・デバイスのうちの少なくとも1つがアクセス・ゲートウェイとの仮想プライベート・ネットワーク接続を確立できない時に、複数のモバイル・デバイスがアクセス・ゲートウェイにアクセスすることを可能にすることを対象とする。

【0006】

たとえば、いくつかの実施形態で、少なくとも2つのモバイル・デバイス（たとえば、第1のモバイル・デバイスおよび第2のモバイル・デバイス）は、それらのデバイスがピアツーピア接続を使用して通信することを可能にする、お互いからのしきい距離以内にある場合がある。さらに、各デバイスは、たとえば、特定のマネージド・アプリケーションがモバイル・デバイス上でどのように実行するのかを制御し、かつ／またはアクセス・ゲートウェイとの仮想プライベート・ネットワーク接続の確立を管理する、企業管理フレームワークを実施するように構成され得る。第1のモバイル・デバイスが、アクセス・ゲートウェイとの仮想プライベート・ネットワーク接続を確立できる場合がある。しかし、第2のモバイル・デバイスは、アクセス・ゲートウェイとのそれ自体の仮想プライベート・ネットワーク接続を確立できない場合がある。したがって、上記に鑑みて、第2のモバイル・デバイスは、第1および第2のモバイル・デバイスがピアツーピア接続を使用するメッシュ・ネットワーク内のメンバになることに基づき、第1のモバイル・デバイスとアクセス・ゲートウェイとの間で確立される仮想プライベート・ネットワーク接続にさらに基づいて、アクセス・ゲートウェイと通信できる可能性がある。

【0007】

実際に、いくつかの実施形態で、第1のモバイル・デバイスは、メッシュ・ネットワークのメンバとしてそれ自体を構成することができる。その構成を完了した後に、第1のモバイル・デバイスは、メッシュ・ネットワーク上でピアツーピア接続を介して第2のモバイル・デバイスと通信できる可能性がある。第1のモバイル・デバイスは、ピアツーピア接続を介して第2のモバイル・デバイスから、アクセス・ゲートウェイ宛のデータを受信

10

20

30

40

50

することができる。第1のモバイル・デバイスは、仮想プライベート・ネットワーク接続を介してアクセス・ゲートウェイにそのデータを送信することができる。

【0008】

上記および追加の態様は、下でさらに詳細に議論される開示の利益に関連付けられる。

【0009】

本明細書で説明される諸態様およびその利益のより完全な理解は、添付図面を考慮して以下の説明を参照することによって獲得され得、図面では、同様の符号が同様の特徴を示す。

【図面の簡単な説明】

【0010】

10

【図1】本明細書で説明される1つまたは複数の例示的な態様に従って使用され得る例示的なコンピュータ・システム・アーキテクチャを示す図である。

【図2】本明細書で説明される1つまたは複数の例示的な態様に従って使用され得る例示的なリモートアクセス・システム・アーキテクチャを示す図である。

【図3】本明細書で説明される1つまたは複数の例示的な態様に従って使用され得る例示的な仮想化された（ハイパーバイザ）システム・アーキテクチャを示す図である。

【図4】本明細書で説明される1つまたは複数の例示的な態様に従って使用され得る例示的なクラウドベースのシステム・アーキテクチャを示す図である。

【図5】例示的な企業モビリティ管理システムを示す図である。

【図6】別の例示的な企業モビリティ管理システムを示す図である。

20

【図7】ユーザが本明細書で説明される様々な態様に従って複数のデバイスを使用して企業リソースおよび企業サービスにアクセスできる可能性がある1つの例の配置を示す図である。

【図8】メッシュ・ネットワークの確立に関連して使用され得る例の方法を示す図である。

【図9】ユーザが本明細書で説明される様々な態様に従って複数のデバイスを使用して企業リソースおよび企業サービスにアクセスできる可能性がある別の例の配置を示す図である。

【図10A】メッシュ・ネットワークの確立に関連して使用され得る別の例の方法を示す図である。

30

【図10B】メッシュ・ネットワークの管理に関連して使用され得る例の方法を示す図である。

【図11A】本明細書で説明される様々な態様に従うメッシュ・ネットワークの使用に関連して使用され得る例の方法を示す図である。

【図11B】本明細書で説明される様々な態様に従うメッシュ・ネットワークの使用に関連して使用され得る例の方法を示す図である。

【図11C】本明細書で説明される様々な態様に従うメッシュ・ネットワークの使用に関連して使用され得る例の方法を示す図である。

【図11D】本明細書で説明される様々な態様に従うメッシュ・ネットワークの使用に関連して使用され得る例の方法を示す図である。

40

【図12】本明細書で説明される態様に従う企業モビリティ管理システムに関連する様々な機能の実行に関連するメッシュ・ネットワークの確立とメッシュ・ネットワークの使用とを示す例のフローを示す図である。

【発明を実施するための形態】

【0011】

様々な実施形態の以下の説明では、上で説明され、本明細書の一部を形成し、実例として本明細書で説明される諸態様を實踐できる様々な実施形態を示す添付図面を参照する。本明細書で説明される範囲から逸脱せずに、他の実施形態が利用され得、構造的変更および機能的変更が行われ得ることを理解されたい。様々な態様は、他の実施形態が可能であり、様々な異なる形で實踐されまたは実行され得る。

50

【0012】

本明細書で使用される語法および用語が、説明のためのものであって限定的とみなされてはならないことを理解されたい。そうではなく、本明細書で使用される句および用語は、その最も広い解釈および意味を与えられなければならない。「含む (including および comprising)」およびその変形の使用は、その後リストされた項目およびその同等物ならびに追加項目およびその同等物の包含を意味する。用語「取り付けられ」、「接続され」、「結合され」、「位置決めされ」、「係合され」、および同様の用語の使用は、直接と間接との両方の取付け、接続、結合、位置決め、および係合を含むことが意図されている。

【0013】

コンピューティング・アーキテクチャ

コンピュータ・ソフトウェア、ハードウェア、およびネットワークは、とりわけ、独立環境、ネットワーク化された環境、リモートアクセス（別名、リモート・デスクトップ）環境、仮想化環境、および／またはクラウドベースの環境を含む様々な異なるシステム環境内で利用され得る。図1は、独立環境および／またはネットワーク化された環境内で本明細書で説明される1つまたは複数の例示的な態様を実施するのに使用され得るシステム・アーキテクチャおよびデータ処理デバイスの一例を示す。様々なネットワーク・ノード103、105、107、および109が、インターネットなどの広域ネットワーク（WAN）101を介して相互接続され得る。プライベート・イントラネット、会社ネットワーク、ローカル・エリア・ネットワーク（LAN）、メトロポリタン・エリア・ネットワーク（MAN）、無線ネットワーク、パーソナル・ネットワーク（PAN）、および類似物を含む他のネットワークが、それに加えてまたはその代わりに使用され得る。ネットワーク101は、例示のためのものであり、より少数または追加のコンピュータ・ネットワークに置換され得る。ローカル・エリア・ネットワーク133は、任意の既知のLANトポロジのうちの1つまたは複数を持つことができ、イーサネット（登録商標）など、様々な異なるプロトコルのうちの1つまたは複数を使用することができる。デバイス103、105、107、および109ならびに他のデバイス（図示せず）は、より対線、同軸ケーブル、光ファイバ、電波、または他の通信媒体を介してネットワークのうちの1つまたは複数に接続され得る。

【0014】

用語「ネットワーク」は、本明細書で使用され、図面に示される時に、リモート・ストレージ・デバイスが1つまたは複数の通信経路を介して一緒に結合されるシステムだけではなく、時々ストレージ能力を有するそのようなシステムに結合され得る独立型デバイスをも指す。その結果、用語「ネットワーク」は、「物理ネットワーク」だけではなく、すべての物理ネットワークにまたがって存在する、単一のエンティティに帰するデータからなる「内容ネットワーク」をも含む。

【0015】

構成要素は、データ・サーバ103、ウェブ・サーバ105、およびクライアント・コンピュータ107、109を含むことができる。データ・サーバ103は、本明細書で説明される1つまたは複数の例示的な態様を実行するためのデータベースおよび制御ソフトウェアの全体的なアクセス、制御、および管理を提供する。データ・サーバ103は、ウェブ・サーバ105に接続され、このウェブ・サーバ105を介して、ユーザは要求通りにデータと対話し、入手する。代替案では、データ・サーバ103は、ウェブ・サーバ自体として働き、インターネットに直接に接続され得る。データ・サーバ103は、ローカル・エリア・ネットワーク133、広域ネットワーク101（たとえば、インターネット）、直接接続もしくは間接接続、またはなんらかの他のネットワークを介してウェブ・サーバ105に接続され得る。ユーザは、リモート・コンピュータ107、109を使用して、たとえば、ウェブ・サーバ105によってホスティングされる1つまたは複数の外部に露出されたウェブ・サイトを介してデータ・サーバ103に接続するのにウェブ・ブラウザを使用して、データ・サーバ103と対話することができる。クライアント・コンピ

ユーザ１０７、１０９は、データ・サーバ１０３に記憶されたデータにアクセスするためにデータ・サーバ１０３と協力して使用され得、または他の目的に使用され得る。たとえば、クライアント・デバイス１０７から、ユーザは、当技術分野で既知のようにインターネット・ブラウザを使用してまたはコンピュータ・ネットワーク（インターネットなど）を介してウェブ・サーバ１０５および／またはデータ・サーバ１０３と通信するソフトウェア・アプリケーションを実行することによって、ウェブ・サーバ１０５にアクセスすることができる。

【００１６】

サーバおよびアプリケーションは、同一の物理計算機上で組み合わせられ、別々の仮想アドレスまたは論理アドレスを保持することができ、あるいは、別々の物理計算機上に存在することができる。図１は、使用され得るネットワーク・アーキテクチャの一例を示すにすぎず、当業者は、本明細書でさらに説明されるように、使用される特定のネットワーク・アーキテクチャおよびデータ処理デバイスが、変化することができ、それらが提供する機能性に対して二次的であることを了解する。たとえば、ウェブ・サーバ１０５およびデータ・サーバ１０３によって提供されるサービスは、単一のサーバ上で組み合わせられ得る。

【００１７】

各構成要素１０３、１０５、１０７、１０９は、任意のタイプの既知のコンピュータ、サーバ、またはデータ処理デバイスとすることができる。たとえば、データ・サーバ１０３は、データ・サーバ１０３の全体的な動作を制御するプロセッサ１１１を含むことができる。データ・サーバ１０３は、ランダム・アクセス・メモリ（RAM）１１３、読取専用メモリ（ROM）１１５、ネットワーク・インターフェース１１７、入出力インターフェース１１９（たとえば、キーボード、マウス、ディスプレイ、プリンタなど）、およびメモリ１２１をさらに含むことができる。入出力（Ｉ／Ｏ）１１９は、データまたはファイルを読み取り、書き込み、表示し、かつ／または印刷する様々なインターフェース・ユニットおよびドライブを含むことができる。メモリ１２１は、データ処理デバイス１０３の全体的な動作を制御するオペレーティング・システム・ソフトウェア１２３、本明細書で説明される諸態様を実行するようにデータ・サーバ１０３に指示する制御論理１２５、ならびに、本明細書で説明される諸態様に関して使用されてもされなくてもよい副機能性、サポート機能性、および／または他の機能性を提供する他のアプリケーション・ソフトウェア１２７をさらに記憶することができる。制御論理は、本明細書ではデータ・サーバ・ソフトウェア１２５と称する場合もある。データ・サーバ・ソフトウェアの機能性は、制御論理にコーディングされたルールに基づいて自動的に行われる動作もしくは判断、ユーザがシステムに入力を供給することによって手動で行われる動作または判断、および／またはユーザ入力（たとえば、クエリ、データ更新など）に基づく自動処理の組み合わせを指すことができる。

【００１８】

メモリ１２１は、第１のデータベース１２９および第２のデータベース１３１を含む、本明細書で説明される１つまたは複数の態様の実行で使用されるデータをも記憶することができる。いくつかの実施形態で、第１のデータベースは、第２のデータベースを含むことができる（たとえば、別々のテーブル、レポートなどとして）。すなわち、情報は、システム設計に応じて、単一のデータベース内に記憶され、または異なる論理データベース、仮想データベース、もしくは物理データベースに分離され得る。デバイス１０５、１０７、および１０９は、デバイス１０３に関して説明されるものに類似するアーキテクチャまたは異なるアーキテクチャを有することができる。当業者は、本明細書で説明されるデータ処理デバイス１０３（または、デバイス１０５、１０７、もしくは１０９）の機能性が、たとえば複数のコンピュータにまたがって処理負荷を分散させる、地理的位置、ユーザ・アクセス・レベル、サービス品質（ＱｏＳ）に基づいてトランザクションを分離するなどのために、複数のデータ処理デバイスにまたがって分配され得ることを了解する。

【００１９】

1つまたは複数の態様は、本明細書で説明される1つまたは複数のコンピュータまたは他のデバイスによって実行される1つまたは複数のプログラム・モジュール内など、コンピュータ使用可能データもしくはコンピュータ可読データおよび／またはコンピュータ実行可能命令内で実施され得る。一般に、プログラム・モジュールは、コンピュータまたは他のデバイス内のプロセッサによって実行された時に特定のタスクを実行しまたは特定の抽象データ型を実施する、ルーチン、プログラム、オブジェクト、コンポーネント、データ構造などを含む。モジュールは、その後に実行のためにコンパイルされるソース・コード・プログラミング言語で記述され得、あるいは、ハイパーテキスト・マークアップ言語（HTML）またはExtensible Markup Language（XML）など（これに限定はされない）のスクリプティング言語で記述され得る。コンピュータ実行可能命令は、不揮発性ストレージ・デバイスなどのコンピュータ可読媒体上に記憶され得る。ハード・ディスク、CD-ROM、光学ストレージ・デバイス、磁気ストレージ・デバイス、および／またはその任意の組み合わせを含む、任意の適切なコンピュータ可読記憶媒体が利用され得る。さらに、本明細書で説明されるデータまたはイベントを表す様々な伝送（非記憶）媒体が、金属ワイヤ、光ファイバ、および／または無線伝送媒体（たとえば、空気および／または空間）などの信号伝導媒体を介して進行する電磁波の形でソースと宛先との間で転送され得る。本明細書で説明される様々な態様は、方法、データ処理システム、またはコンピュータ・プログラム製品として実施され得る。したがって、様々な機能性は、全体的にまたは部分的にソフトウェアで、ファームウェアで、ならびに／または集積回路、フィールド・プログラマブル・ゲート・アレイ（FPGA）、および類似物などのハードウェアもしくはハードウェア同等物で実施され得る。特定のデータ構造が、本明細書で説明される1つまたは複数の態様をより効率的に実施するのに使用され得、そのようなデータ構造は、本明細書で説明されるコンピュータ実行可能命令およびコンピュータ使用可能データの範囲内で企図されている。

【0020】

図2をさらに参照すると、本明細書で説明される1つまたは複数の態様は、リモートアクセス環境内で実施され得る。図2は、本明細書で説明される1つまたは複数の例示的な諸態様に従って使用され得る例示的なコンピューティング環境200内の一般的なコンピューティング・デバイス201を含む例のシステム・アーキテクチャを示す。一般的なコンピューティング・デバイス201は、クライアント・アクセス・デバイスに仮想計算機を提供するように構成されたシングルサーバまたはマルチサーバのデスクトップ仮想化システム（たとえば、リモートアクセス・システムまたはクラウド・システム）内のサーバ206aとして使用され得る。一般的なコンピューティング・デバイス201は、サーバと、RAM 205、ROM 207、入出力（I/O）モジュール209、およびメモリ215を含むそれに関連する構成要素との全体的な動作を制御するプロセッサ203を有することができる。

【0021】

I/Oモジュール209は、それを介して一般的なコンピューティング・デバイス201のユーザが入力を供給できるマウス、キーパッド、タッチ・スクリーン、スキャナ、光学リーダー、および／またはスタイラス（または他の入力デバイス（1つまたは複数））を含むことができ、オーディオ出力を提供する1つまたは複数のスピーカならびにテキスト出力、オーディオビジュアル出力、および／またはグラフィカル出力を提供する1つまたは複数のビデオ・ディスプレイ・デバイスを含むこともできる。ソフトウェアは、本明細書で説明される様々な機能を実行するために一般的なコンピューティング・デバイス201を特殊目的コンピューティング・デバイスに構成するためにプロセッサ203に命令を供給するためにメモリ215および／または他のストレージ内に記憶され得る。たとえば、メモリ215は、オペレーティング・システム217、アプリケーション・プログラム219、および関連するデータベース221など、コンピューティング・デバイス201によって使用されるソフトウェアを記憶することができる。

【0022】

10

20

30

40

50

コンピューティング・デバイス 201 は、端末 240（クライアント・デバイスとも称する）など、1 つまたは複数のリモート・コンピュータへの接続をサポートするネットワーク化された環境内で動作することができる。端末 240 は、上で一般的なコンピューティング・デバイス 103 または 201 に関して説明した要素の多数またはすべてを含むパーソナル・コンピュータ、モバイル・デバイス、ラップトップ・コンピュータ、タブレット、またはサーバとすることができる。図 2 に示されたネットワーク接続は、ローカル・エリア・ネットワーク（LAN）225 および広域ネットワーク（WAN）229 を含むが、他のネットワークを含むこともできる。LAN ネットワーキング環境で使用される時に、コンピューティング・デバイス 201 は、ネットワーク・インターフェースまたはネットワーク・アダプタ 223 を介して LAN 225 に接続され得る。WAN ネットワーキング環境で使用される時に、コンピューティング・デバイス 201 は、コンピュータ・ネットワーク 230（たとえば、インターネット）などの WAN 229 を介する通信を確立するモデム 227 または他の広域ネットワーク・インターフェースを含むことができる。図示のネットワーク接続が、例示であり、コンピュータの間の通信リンクを確立する他の手段が使用され得ることを了解されたい。コンピューティング・デバイス 201 および／または端末 240 は、バッテリー、スピーカ、およびアンテナ（図示せず）などの様々な他の構成要素を含むモバイル端末（たとえば、携帯電話機、スマート・フォン、携帯情報端末（PDA）、ノートブックなど）とすることもできる。

【0023】

本明細書で説明される態様は、多数の他の汎用または特殊目的のコンピューティング・システム環境またはコンピューティング・システム構成と共に動作することもできる。本明細書で説明される態様と共に使用するのに適する可能性がある他のコンピューティング・システム、環境、および／または構成の例は、パーソナル・コンピュータ、サーバ・コンピュータ、ハンドヘルド・デバイス、ラップトップ・デバイス、マルチプロセッサ・システム、マイクロプロセッサベースのシステム、セット・トップ・ボックス、プログラム可能な消費者エレクトロニクス、ネットワーク・パーソナル・コンピュータ（PC）、ミニコンピュータ、メインフレーム・コンピュータ、上記のシステムまたはデバイスのいずれかを含む分散コンピューティング環境、および類似物を含むが、これに限定されない。

【0024】

図 2 に示されているように、1 つまたは複数のクライアント・デバイス 240 は、1 つまたは複数のサーバ 206a～206n（本明細書では全体的に「サーバ（1 つまたは複数）206」と称する）と通信しているものとすることができる。一実施形態では、コンピューティング環境 200 は、サーバ（1 つまたは複数）206 とクライアント計算機（1 つまたは複数）240 との間に設置されたネットワーク・アプライアンスを含むことができる。ネットワーク・アプライアンスは、クライアント／サーバ接続を管理することができ、いくつかの場合に、複数のバックエンド・サーバ 206 の中でクライアント接続の負荷を平衡化することができる。

【0025】

クライアント計算機（1 つまたは複数）240 は、いくつかの実施形態で、単一のクライアント計算機 240 またはクライアント計算機 240 の単一のグループと呼ばれる場合があり、サーバ（1 つまたは複数）206 は、単一のサーバ 206 またはサーバ 206 の単一のグループと呼ばれる場合がある。一実施形態では、単一のクライアント計算機 240 が、複数のサーバ 206 と通信し、別の実施形態では、単一のサーバ 206 が、複数のクライアント計算機 240 と通信する。さらに別の実施形態では、単一のクライアント計算機 240 が単一のサーバ 206 と通信する。

【0026】

クライアント計算機 240 は、いくつかの実施形態で、クライアント計算機（1 つまたは複数）、クライアント（1 つまたは複数）、クライアント・コンピュータ（1 つまたは複数）、クライアント・デバイス（1 つまたは複数）、クライアント・コンピューティング・デバイス（1 つまたは複数）、ローカル計算機、リモート計算機、クライアント・ノ

ード（１つまたは複数）、エンドポイント（１つまたは複数）、またはエンドポイント・ノード（１つまたは複数）という非網羅的な項目のうちの任意の１つによって参照され得る。サーバ２０６は、いくつかの実施形態で、サーバ（１つまたは複数）、ローカル計算機、リモート計算機、サーバ・ファーム（１つまたは複数）、またはホスト・コンピューティング・デバイス（１つまたは複数）という非網羅的な項目のうちの任意の１つによって参照され得る。

【００２７】

一実施形態では、クライアント計算機２４０は、仮想計算機とすることができる。仮想計算機は、任意の仮想計算機とすることができるが、いくつかの実施形態では、仮想計算機は、タイプ１またはタイプ２のハイパーバイザ、たとえばCitrix Systems、IBM、VMwareによって開発されたハイパーバイザまたは任意の他のハイパーバイザによって管理される任意の仮想計算機とすることができる。いくつかの態様では、仮想計算機は、ハイパーバイザによって管理され得、他の態様では、仮想計算機は、サーバ２０６上で実行するハイパーバイザまたはクライアント２４０上で実行するハイパーバイザによって管理され得る。

【００２８】

いくつかの実施形態は、サーバ２０６または他のリモートに配置された計算機上でリモートに実行するアプリケーションによって生成されたアプリケーション出力を表示するクライアント・デバイス２４０を含む。これらの実施形態では、クライアント・デバイス２４０は、アプリケーション・ウィンドウ、ブラウザ、または他の出力ウィンドウ内に出力を表示するために仮想計算機受信器プログラムまたはアプリケーションを実行することができる。一例では、アプリケーションは、デスクトップであるが、他の例では、アプリケーションは、デスクトップを生成しまたは提示するアプリケーションである。デスクトップは、ローカル・アプリケーションおよび／またはリモート・アプリケーションがその中で統合され得るオペレーティング・システムのインスタンスのユーザ・インターフェースを提供するグラフィカル・シェルを含むことができる。アプリケーションは、本明細書で使用される時に、オペレーティング・システムのインスタンスが（および、オプションでデスクトップも）ロードされた後に実行するプログラムである。

【００２９】

サーバ２０６は、いくつかの実施形態で、サーバ２０６でのアプリケーション実行によって生成されたディスプレイ出力を提示するためにクライアント上で実行するシンクライアント・アプリケーションまたはリモートディスプレイ・アプリケーションにデータを送るのにリモート・プレゼンテーション・プロトコルまたは他のプログラムを使用する。シンクライアント・プロトコルまたはリモートディスプレイ・プロトコルは、米国フロリダ州フォート・ローダーデールのCitrix Systems, Inc.によって開発されたIndependent Computing Architecture (ICA) プロトコルまたは米国ワシントン州レッドモンドのMicrosoft Corporationによって製造されるRemote Desktop Protocol (RDP) というプロトコルの非網羅的なリストのうちの任意の１つとすることができる。

【００３０】

リモート・コンピューティング環境は、サーバ２０６a～２０６nがたとえばクラウド・コンピューティング環境内でサーバ・ファーム２０６に論理的に一緒にグループ化されるように、複数のサーバ２０６a～２０６nを含むことができる。サーバ・ファーム２０６は、論理的に一緒にグループ化される間に地理的に分散されるサーバ２０６または論理的に一緒にグループ化される間にお互いに近接して配置されるサーバ２０６を含むことができる。サーバ・ファーム２０６内の地理的に分散されたサーバ２０６a～２０６nは、いくつかの実施形態で、WAN（広域）、MAN（メトロポリタン）、またはLAN（ローカル）を使用して通信することができ、異なる地理的領域は、異なる大陸、１つの大陸の異なる領域、異なる国、異なる州、異なる都市、異なるキャンパス、異なる部屋、または先行する地理的位置の任意の組み合わせとして特徴を表され得る。いくつかの実施形態

で、サーバ・ファーム 206 は、単一のエンティティとして管理され得、他の実施形態では、サーバ・ファーム 206 は、複数のサーバ・ファームを含むことができる。

【0031】

いくつかの実施形態で、サーバ・ファームは、実質的に類似するタイプのオペレーティング・システム・プラットフォーム（たとえば、WINDOWS（登録商標）、UNIX（登録商標）、LINUX、iOS、ANDROID（登録商標）、SYMBIANなど）を実行するサーバ 206 を含むことができる。他の実施形態では、サーバ・ファーム 206 は、第 1 のタイプのオペレーティング・システム・プラットフォームを実行する 1 つまたは複数のサーバの第 1 のグループと、第 2 のタイプのオペレーティング・システム・プラットフォームを実行する 1 つまたは複数のサーバの第 2 のグループとを含むことができる。

10

【0032】

サーバ 206 は、必要に応じて、任意のタイプのサーバとして、たとえばファイル・サーバ、アプリケーション・サーバ、ウェブ・サーバ、プロキシ・サーバ、アプライアンス、ネットワーク・アプライアンス、ゲートウェイ、アプリケーション・ゲートウェイ、ゲートウェイ・サーバ、仮想化サーバ、展開サーバ、Secure Sockets Layer (SSL) VPNサーバ、ファイヤウォール、ウェブ・サーバ、アプリケーション・サーバもしくはマスタ・アプリケーション・サーバ、アクティブ・ディレクトリを実行するサーバ、または、ファイヤウォール機能性、アプリケーション機能性、もしくは負荷平衡化機能性を提供するアプリケーション加速プログラムを実行するサーバとして構成され得る。他のサーバ・タイプも使用され得る。

20

【0033】

いくつかの実施形態は、クライアント計算機 240 から要求を受信し、第 2 のサーバ 206 b（図示せず）に要求を転送し、第 2 のサーバ 206 b（図示せず）からの応答を用いて、クライアント計算機 240 によって生成された要求に応答する、第 1 のサーバ 206 a を含む。第 1 のサーバ 206 a は、クライアント計算機 240 から使用可能なアプリケーションの列挙およびアプリケーションの列挙内で識別されたアプリケーションをホスティングするアプリケーション・サーバ 206 に関連するアドレス情報をも獲得することができる。第 1 のサーバ 206 a は、その後、ウェブ・インターフェースを使用してクライアントの要求に対する応答を提示し、識別されたアプリケーションへのアクセスをクライアント 240 に提供するためにクライアント 240 と直接に通信することができる。1 つまたは複数のクライアント 240 および／または 1 つまたは複数のサーバ 260 が、ネットワーク 230、たとえばネットワーク 101 を介してデータを送信することができる。

30

【0034】

図 3 は、例示的なデスクトップ仮想化システムの高水準アーキテクチャを示す。図示されているように、デスクトップ仮想化システムは、仮想デスクトップおよび／または仮想アプリケーションを 1 つまたは複数のクライアント・アクセス・デバイス 240 に提供するように構成された少なくとも 1 つの仮想化サーバ 301 を含む、シングルサーバ・システムもしくはマルチサーバ・システム、またはクラウド・システムとすることができる。本明細書で使用される時に、デスクトップは、1 つまたは複数のアプリケーションがホスティングされ、かつ／または実行され得るグラフィカル環境または空間を指す。デスクトップは、ローカル・アプリケーションおよび／またはリモート・アプリケーションがその中で統合され得るオペレーティング・システムのインスタンスにユーザ・インターフェースを提供するグラフィカル・シェルを含むことができる。アプリケーションは、オペレーティング・システムのインスタンスが（および、オプションでデスクトップも）ロードされた後に実行されるプログラムを含むことができる。オペレーティング・システムの各インスタンスは、物理的（たとえば、1 デバイスあたり 1 つのオペレーティング・システム）または仮想（たとえば、単一のデバイス上で走行する 1 つの OS の多数のインスタンス）とすることができる。各アプリケーションは、ローカル・デバイス上で実行され、また

40

50

はリモートに配置されたデバイス（たとえば、遠隔化された）上で実行され得る。

【0035】

コンピュータ・デバイス301は、仮想化環境、たとえばシングルサーバ環境、マルチサーバ環境、またはクラウド・コンピューティング環境内の仮想化サーバとして構成され得る。図3に示された仮想化サーバ301は、図2に示されたサーバ206の1つまたは複数の実施形態または他の既知のコンピューティング・デバイスとして展開され、かつ／またはこれによって実施され得る。仮想化サーバ301内に含まれるのは、1つまたは複数の物理ディスク304、1つまたは複数の物理デバイス306、1つまたは複数の物理プロセッサ308、および1つまたは複数の物理メモリ316を含むことのできるハードウェア層である。いくつかの実施形態では、ファームウェア312は、物理メモリ316内のメモリ要素内に記憶され得、物理プロセッサ308のうちの1つまたは複数によって実行され得る。仮想化サーバ301は、物理メモリ316内のメモリ要素内に記憶され、物理プロセッサ308のうちの1つまたは複数によって実行され得るオペレーティング・システム314をさらに含むことができる。さらに、ハイパーバイザ302が、物理メモリ316内のメモリ要素内に記憶され得、物理プロセッサ308のうちの1つまたは複数によって実行され得る。

10

【0036】

物理プロセッサ308のうちの1つまたは複数上で実行しているのは、1つまたは複数の仮想計算機332A～C（全体的に332）とすることができる。各仮想計算機332は、仮想ディスク326A～Cおよび仮想プロセッサ328A～Cを有することができる。いくつかの実施形態で、第1の仮想計算機332Aは、仮想プロセッサ328Aを使用して、ツール・スタック324を含む制御プログラム320を実行することができる。制御プログラム320は、制御仮想計算機、Dom0、ドメイン0、またはシステム管理および／もしくはシステム制御に使用される他の仮想計算機と呼ばれる場合がある。いくつかの実施形態では、1つまたは複数の仮想計算機332B～Cは、仮想プロセッサ328B～Cを使用して、ゲスト・オペレーティング・システム330A～Bを実行することができる。

20

【0037】

仮想化サーバ301は、仮想化サーバ301と通信する1つまたは複数のハードウェアを有するハードウェア層310を含むことができる。いくつかの実施形態で、ハードウェア層310は、1つまたは複数の物理ディスク304、1つまたは複数の物理デバイス306、1つまたは複数の物理プロセッサ308、および1つまたは複数の物理メモリ316を含むことができる。物理構成要素304、306、308、および316は、たとえば、上で説明された構成要素のいずれかを含むことができる。物理デバイス306は、たとえば、ネットワーク・インターフェース・カード、ビデオ・カード、キーボード、マウス、入力デバイス、モニタ、ディスプレイ・デバイス、スピーカ、光学ドライブ、ストレージ・デバイス、universal serial bus接続、プリンタ、スキャナ、ネットワーク要素（たとえば、ルータ、ファイヤウォール、ネットワーク・アドレス・トランスレータ、ロード・バランサ、仮想プライベート・ネットワーク（VPN）ゲートウェイ、動的ホスト構成プロトコル（DHCP）ルータなど）、または仮想化サーバ301に接続されもしくはこれと通信する任意のデバイスを含むことができる。ハードウェア層310内の物理メモリ316は、任意のタイプのメモリを含むことができる。物理メモリ316は、データを記憶することができ、いくつかの実施形態では、1つもしくは複数のプログラムまたは実行可能命令のセットを記憶することができる。図3は、ファームウェア312が仮想化サーバ301の物理メモリ316内に記憶される実施形態を示す。物理メモリ316内に記憶されたプログラムまたは実行可能命令は、仮想化サーバ301の1つまたは複数のプロセッサ308によって実行され得る。

30

40

【0038】

仮想化サーバ301は、ハイパーバイザ302をも含むことができる。いくつかの実施形態で、ハイパーバイザ302は、任意の個数の仮想計算機332を作成し、管理するた

50

めに仮想化サーバ301上でプロセッサ308によって実行されるプログラムとすることができる。ハイパーバイザ302は、仮想計算機モニタまたはプラットフォーム仮想化ソフトウェアと呼ばれる場合がある。いくつかの実施形態では、ハイパーバイザ302は、実行可能命令と、コンピューティング機械上で実行する仮想計算機を監視するハードウェアとの任意の組み合わせとすることができる。ハイパーバイザ302は、ハイパーバイザが仮想化サーバ301上で実行するオペレーティング・システム314内で実行する、タイプ2ハイパーバイザとすることができる。仮想計算機は、ハイパーバイザの上のレベルで実行することができる。いくつかの実施形態では、タイプ2ハイパーバイザは、タイプ2ハイパーバイザがユーザのオペレーティング・システムと相互作用するように、ユーザのオペレーティング・システムのコンテキスト内で実行することができる。他の実施形態では、仮想化環境内の1つまたは複数の仮想化サーバ301は、その代わりにタイプ1ハイパーバイザ（図示せず）を含むことができる。タイプ1ハイパーバイザは、ハードウェア層310内のハードウェアおよびリソースに直接にアクセスすることによって仮想化サーバ301上で実行することができる。すなわち、タイプ2ハイパーバイザ302は、図示のようにホスト・オペレーティング・システム314を介してシステム・リソースにアクセスするが、タイプ1ハイパーバイザは、ホスト・オペレーティング・システム314なしですべてのシステム・リソースに直接にアクセスすることができる。タイプ1ハイパーバイザは、仮想化サーバ301の1つまたは複数の物理プロセッサ308上で直接に実行することができ、物理メモリ316内に記憶されたプログラム・データを含むことができる。

10

20

【0039】

ハイパーバイザ302は、いくつかの実施形態で、システム・リソースへの直接アクセスを有するオペレーティング・システム330または制御プログラム320をシミュレートする任意の形で仮想計算機332上で実行するオペレーティング・システム330または制御プログラム320に仮想リソースを提供することができる。システム・リソースは、物理デバイス306、物理ディスク304、物理プロセッサ308、物理メモリ316、および仮想化サーバ301ハードウェア層310内に含まれる任意の他の構成要素を含むことができるが、これに限定はされない。ハイパーバイザ302は、仮想ハードウェアをエミュレートし、物理ハードウェアを区分し、物理ハードウェアを仮想化し、かつ／またはコンピューティング環境へのアクセスを提供する仮想計算機を実行するのに使用され得る。さらに他の実施形態では、ハイパーバイザ302は、仮想化サーバ301上で実行する仮想計算機332のプロセッサ・スケジューリングおよびメモリ・パーティショニングを制御することができる。ハイパーバイザ302は、米国カリフォルニア州パロ・アルトのVMWare, Inc.によって製造されるもの、その開発がオープン・ソースXenProject.orgコミュニティによって監督されるオープン・ソース・プロジェクトであるXENPROJECTハイパーバイザ、Microsoftによって提供されるHyperV、VirtualServer、またはvirtual PCハイパーバイザ、その他を含むことができる。いくつかの実施形態で、仮想化サーバ301は、ゲスト・オペレーティング・システムがその上で実行できる仮想計算機プラットフォームを作成するハイパーバイザ302を実行することができる。これらの実施形態では、仮想化サーバ301が、ホスト・サーバと呼ばれる場合がある。そのような仮想化サーバの例は、米国フロリダ州フォート・ローダーデールのCitrix Systems, Inc.によって提供されるXENSERVRである。

30

40

【0040】

ハイパーバイザ302は、その中でゲスト・オペレーティング・システム330が実行する1つまたは複数の仮想計算機332B~C（全体的に332）を作成することができる。いくつかの実施形態で、ハイパーバイザ302は、仮想計算機332を作成するために仮想計算機イメージをロードすることができる。他の実施形態では、ハイパーバイザ302は、仮想計算機332内でゲスト・オペレーティング・システム330を実行することができる。さらなる他の実施形態では、仮想計算機332がゲスト・オペレーティング

50

・システム 330 を実行することができる。

【0041】

仮想計算機 332 の作成に加えて、ハイパーバイザ 302 は、少なくとも 1 つの仮想計算機 332 の実行を制御することができる。他の実施形態では、ハイパーバイザ 302 は、仮想化サーバ 301 によって提供される少なくとも 1 つのハードウェア・リソース（たとえば、ハードウェア層 310 内で使用可能な任意のハードウェア・リソース）の抽象化を用いて少なくとも 1 つの仮想計算機 332 を提示することができる。他の実施形態では、ハイパーバイザ 302 は、仮想計算機 332 が仮想化サーバ 301 内で使用可能な物理プロセッサ 308 にアクセスする形を制御することができる。物理プロセッサ 308 へのアクセスの制御は、仮想計算機 332 がプロセッサ 308 へのアクセスを有するべきかどうかと、物理プロセッサ能力が仮想計算機 332 にどのように提示されるのかとを判定することを含むことができる。

10

【0042】

図 3 に示されているように、仮想化サーバ 301 は、1 つまたは複数の仮想計算機 332 をホスティングしまたは実行することができる。仮想計算機 332 は、プロセッサ 308 によって実行された時に、仮想計算機 332 が物理コンピューティング・デバイスのようにプログラムおよびプロセスを実行できるように物理コンピュータの動作を模倣することのできる実行可能命令のセットである。図 3 は、仮想化サーバ 301 が 3 つの仮想計算機 332 をホスティングする実施形態を示すが、他の実施形態では、仮想化サーバ 301 は、任意の個数の仮想計算機 332 をホスティングすることができる。ハイパーバイザ 302 は、いくつかの実施形態で、各仮想計算機 332 に、その仮想計算機 332 が使用可能な物理ハードウェア、メモリ、プロセッサ、および他のシステム・リソースの独自の仮想ビューを提供することができる。いくつかの実施形態では、独自の仮想ビューは、仮想計算機アクセス権、1 つまたは複数の仮想計算機識別子へのポリシー・エンジンの適用、仮想計算機にアクセスするユーザ、仮想計算機上で実行中のアプリケーション、仮想計算機によってアクセスされるネットワーク、または任意の他の所望の判断基準のうちの 1 つまたは複数に基づくものとすることができる。たとえば、ハイパーバイザ 302 は、1 つまたは複数の非セキュア仮想計算機 332 および 1 つまたは複数のセキュア仮想計算機 332 を作成することができる。非セキュア仮想計算機 332 は、セキュア仮想計算機 332 がアクセスを許可されるリソース、ハードウェア、メモリ位置、およびプログラムへのアクセスを防止され得る。他の実施形態では、ハイパーバイザ 302 は、各仮想計算機 332 に、仮想計算機 332 からアクセス可能な物理ハードウェア、メモリ、プロセッサ、および他のシステム・リソースの実質的に同様の仮想ビューを提供することができる。

20

30

【0043】

各仮想計算機 332 は、仮想ディスク 326 A～C（全体的に 326）および仮想プロセッサ 328 A～C（全体的に 328）を含むことができる。仮想ディスク 326 は、いくつかの実施形態で、仮想化サーバ 301 の 1 つまたは複数の物理ディスク 304 または仮想化サーバ 301 の 1 つまたは複数の物理ディスク 304 の一部の仮想化されたビューである。物理ディスク 304 の仮想化されたビューは、ハイパーバイザ 302 によって生成され、提供され、管理され得る。いくつかの実施形態で、ハイパーバイザ 302 は、各仮想計算機 332 に物理ディスク 304 の独自のビューを提供する。したがって、これらの実施形態では、各仮想計算機 332 に含まれる特定の仮想ディスク 326 は、他の仮想ディスク 326 と比較した時に独自とすることができる。

40

【0044】

仮想プロセッサ 328 は、仮想化サーバ 301 の 1 つまたは複数の物理プロセッサ 308 の仮想化されたビューとすることができる。いくつかの実施形態で、物理プロセッサ 308 の仮想化されたビューは、ハイパーバイザ 302 によって生成され、提供され、管理され得る。いくつかの実施形態で、仮想プロセッサ 328 は、少なくとも 1 つの物理プロセッサ 308 の同一の特性の実質的にすべてを有する。他の実施形態では、仮想プロセッサ 308 は、仮想プロセッサ 328 の特性のうちの少なくとも一部が、対応する物理プロ

50

セッサ 308 の特性とは異なるように、物理プロセッサ 308 の変更されたビューを提供する。

【0045】

図 4 をさらに参照すると、本明細書で説明されるいくつかの態様は、クラウドベースの環境内で実施され得る。図 4 は、クラウド・コンピューティング環境（またはクラウド・システム）400 の一例を示す。図 4 からわかるように、クライアント・コンピュータ 411～414 は、クラウド・システムのコンピューティング・リソース（たとえば、ホスト・サーバ 403 a～403 b（本明細書では全体的に「ホスト・サーバ 403」と称する）、ストレージ・リソース 404 a～404 b（本明細書では全体的に「ストレージ・リソース 404」と称する）、およびネットワーク・リソース 405 a～405 b（本明細書では全体的に「ネットワーク・リソース 405」と称する））にアクセスするためにクラウド管理サーバ 410 と通信することができる。

10

【0046】

管理サーバ 410 は、1 つまたは複数の物理サーバ上で実施され得る。管理サーバ 410 は、たとえば、とりわけ米国フロリダ州フォート・ローダーデールの Citrix Systems, Inc. による CLOUDPLATFORM または OPENSTACK を走行させることができる。管理サーバ 410 は、クラウド・ハードウェア・リソースおよびクラウド・ソフトウェア・リソース、たとえば、ホスト・コンピュータ 403、データ・ストレージ・デバイス 404、およびネットワークング・デバイス 405 を含む様々なコンピューティング・リソースを管理することができる。クラウド・ハードウェア・リソースおよびクラウド・ソフトウェア・リソースは、私有構成要素および／または公衆構成要素を含むことができる。たとえば、クラウドは、1 つまたは複数の特定の顧客もしくはクライアント・コンピュータ 411～414 によっておよび／または私有ネットワーク上で使用される私有クラウドとして構成され得る。他の実施形態では、公衆クラウドまたはハイブリッド公衆／私有クラウドが、オープン・ネットワークまたはハイブリッド・ネットワークを介して他の顧客によって使用され得る。

20

【0047】

管理サーバ 410 は、それを介してクラウド・オペレータおよびクラウド顧客がクラウド・システム 400 と対話できるユーザ・インターフェースを提供するように構成され得る。たとえば、管理サーバ 410 は、クラウド・オペレータがクラウド・リソースを管理し、仮想化層を構成し、顧客アカウントを管理し、他のクラウド管理タスクを実行することを可能にするために、アプリケーション・プログラミング・インターフェース（API）のセットおよび／または 1 つもしくは複数のクラウド・オペレータ・コンソール・アプリケーション（たとえば、ウェブ・ベースのまたは独立型のアプリケーション）にユーザ・インターフェースを提供することができる。管理サーバ 410 は、クライアント・コンピュータ 411～414 を介してエンド・ユーザからクラウド・コンピューティング要求、たとえばクラウド内で仮想計算機を作成し、変更し、または破壊する要求を受信するように構成されたユーザ・インターフェースを有する API のセットおよび／または 1 つもしくは複数の顧客コンソール・アプリケーションを含むこともできる。クライアント・コンピュータ 411～414 は、インターネットまたはなんらかの他の通信ネットワークを介して管理サーバ 410 に接続することができ、管理サーバ 410 によって管理されるコンピューティング・リソースのうちの 1 つまたは複数へのアクセスを要求することができる。クライアント要求に応答して、管理サーバ 410 は、クライアント要求に基づいてクラウド・システムのハードウェア層内の物理リソースを選択し、提供するように構成されたリソース・マネージャを含むことができる。たとえば、管理サーバ 410 およびクラウド・システムの追加構成要素は、ネットワーク（たとえば、インターネット）を介してクライアント・コンピュータ 411～414 の顧客に仮想計算機およびその動作環境（たとえば、ハイパーバイザ、ストレージ・リソース、ネットワーク要素によって提供されるサービスなど）を提供し、作成し、管理し、計算リソース、データ・ストレージ・サービス、ネットワーク能力、ならびにコンピュータ・プラットフォームおよびアプリケーシ

30

40

50

ョン・サポートを提供するように構成され得る。クラウド・システムは、セキュリティ・サービス、展開環境、ユーザ・インターフェース、および類似物を含む様々な特定のサービスを提供するようにも構成され得る。

【0048】

クライアント・コンピュータ411～414は、たとえば、同一のエンド・ユーザまたは同一の会社もしくは組織に加入した異なるユーザの代わりに仮想計算機を作成する異なるクライアント・コンピュータに関するものとして行うことができる。他の例では、ある種のクライアント411～414は、異なる会社または組織に加入したユーザなど、関係しないものとして行うことができる。関係しないクライアントに関して、任意のユーザの仮想計算機またはストレージ上の情報は、他のユーザから隠蔽され得る。

10

【0049】

ここでクラウド・コンピューティング環境の物理ハードウェア層を参照すると、可用性ゾーン401～402（またはゾーン）は、物理コンピューティング・リソースの同一位置に配置されたセットを指すことができる。ゾーンは、コンピューティング・リソースの全体的なクラウド内で他のゾーンから地理的に分離され得る。たとえば、ゾーン401は、米国カリフォルニア州に配置された第1のクラウド・データセンタとすることができ、ゾーン402は、米国フロリダ州に配置された第2のクラウド・データセンタとすることができる。管理サーバ410は、可用性ゾーンのうちの1つまたは別々の位置に配置され得る。各ゾーンは、ゲートウェイを介して、管理サーバ410などのゾーンの外部のデバイスとインターフェースする内部ネットワークを含むことができる。クラウドのエンド・ユーザ（たとえば、クライアント411～414）は、ゾーンの間の区別を知っていてもいなくてもよい。たとえば、エンド・ユーザは、指定された量のメモリ、処理能力、およびネットワーク能力を有する仮想計算機の作成を要求することができる。管理サーバ410は、ユーザの要求に応答することができ、仮想計算機がゾーン401またはゾーン402のどちらからのリソースを使用して作成されたのかをユーザが知ることなく、仮想計算機を作成するためにリソースを割り振ることができる。他の例では、クラウド・システムは、仮想計算機（または他のクラウド・リソース）が特定のゾーン内またはあるゾーン内の特定のリソース403～405上で割り振られることをエンド・ユーザが要求することを可能にすることができる。

20

【0050】

この例では、各ゾーン401～402は、様々な物理ハードウェア構成要素（またはコンピューティング・リソース）403～405、たとえば、物理ホスティング・リソース（または処理リソース）、物理ネットワーク・リソース、物理ストレージ・リソース、スイッチ、およびクラウド・コンピューティング・サービスを顧客に提供するのに使用され得る追加のハードウェア・リソースの配置を含むことができる。クラウド・ゾーン401～402内の物理ホスティング・リソースは、上で説明した仮想化サーバ301など、仮想計算機インスタンスを作成し、ホスティングするように構成され得る1つまたは複数のコンピュータ・サーバ403を含むことができる。クラウド・ゾーン401または402内の物理ネットワーク・リソースは、ファイヤウォール、ネットワーク・アドレス・トランスレータ、ロード・バランサ、仮想プライベート・ネットワーク（VPN）ゲートウェイ、動的ホスト構成プロトコル（DHCP）ルータ、および類似物など、クラウド顧客にネットワーク・サービスを提供するように構成されたハードウェアおよび／またはソフトウェアを含む1つまたは複数のネットワーク要素405（たとえば、ネットワーク・サービス・プロバイダを含むことができる。クラウド・ゾーン401～402内のストレージ・リソースは、ストレージ・ディスク（たとえば、ソリッド・ステート・ドライブ（SSD）、磁気ハード・ディスクなど）および他のストレージ・デバイスを含むことができる。

30

40

【0051】

図4に示された例のクラウド・コンピューティング環境は、仮想計算機を作成し、管理し、クラウド内の物理リソースを使用して顧客に他のサービスを提供するように構成され

50

た追加のハードウェア・リソースおよび／またはソフトウェア・リソースを有する仮想化層（たとえば、図1～図3に示された）をも含むことができる。仮想化層は、ネットワーク仮想化、ストレージ仮想化などを提供する他の構成要素と一緒に、上で図3で説明したハイパーバイザを含むことができる。仮想化層は、物理リソース層とは別々の層として存在することができ、あるいは、同一のハードウェア・リソースおよび／またはソフトウェア・リソースの一部またはすべてを物理リソース層と共有することができる。たとえば、仮想化層は、物理コンピューティング・リソースと共に仮想化サーバ403のそれぞれにインストールされたハイパーバイザを含むことができる。その代わりに、既知のクラウド・システム、たとえばWINDOWS（登録商標）AZURE（米国ワシントン州レッドモンドのMicrosoft Corporation）、AMAZON EC2（米国ワシントン州シアトルのAmazon.com Inc.）、IBM BLUE CLOUD（米国ニューヨーク州アーモンのIBM Corporation）、その他を使用することができる。

【0052】

企業モビリティ管理アーキテクチャ

図5は、「Bring Your Own Device」（BYOD）環境で使用される企業モビリティ技術アーキテクチャ500を表す。このアーキテクチャは、モバイル・デバイス502のユーザが、モバイル・デバイス502から企業リソースまたは個人リソースにアクセスすることと、個人的使用のためにモバイル・デバイス502を使用することとの両方を可能にする。ユーザは、ユーザによって購入されたモバイル・デバイス502または企業によってユーザに提供されたモバイル・デバイス502を使用して、そのような企業リソース504または企業サービス508にアクセスすることができる。ユーザは、業務専用または業務と個人使用とにモバイル・デバイス502を利用することができる。モバイル・デバイス502は、iOSオペレーティング・システム、Android（登録商標）オペレーティング・システム、または類似物を走行させることができる。企業は、モバイル・デバイス502を管理するためにポリシーを実施することを選択することができる。ポリシーは、モバイル・デバイス502が識別され、保護されまたはセキュリティ検証され、企業リソース（たとえば、504および508）への選択的アクセスまたはフル・アクセスを提供され得るような形でファイヤウォールまたはゲートウェイを介して実施され得る。ポリシーは、モバイル・デバイス管理ポリシー、モバイル・アプリケーション管理ポリシー、モバイル・データ管理ポリシー、またはモバイル・デバイス管理ポリシー、モバイル・アプリケーション管理ポリシー、およびモバイル・データ管理ポリシーのなんらかの組み合わせとすることができる。モバイル・デバイス管理ポリシーの適用を介して管理されるモバイル・デバイス502は、登録されたデバイスと呼ばれる場合がある。

【0053】

いくつかの実施形態で、モバイル・デバイス502のオペレーティング・システムは、管理されるパーティション510および管理されないパーティション512に分離される。管理されるパーティション510は、管理されるパーティション510上で走行するアプリケーションおよび管理されるパーティション510内に記憶されるデータを保護するためにポリシーを適用され得る。管理されるパーティション510上で走行するアプリケーションは、セキュア・アプリケーションとすることができる。他の実施形態では、すべてのアプリケーションが、アプリケーションとは別々に受信され、1つまたは複数のセキュリティ・パラメータ、特徴、リソース制限、および／またはアプリケーションがモバイル・デバイス502上で実行している時にモバイル・デバイス管理システムによって実施される他のアクセス制御を定義する、1つまたは複数のポリシー・ファイルのセットに従って実行することができる。そのそれぞれのポリシー・ファイル（1つまたは複数）に従って動作することによって、各アプリケーションは、1つまたは複数の他のアプリケーションおよび／またはリソースとの通信を許可されまたは制限され、これによって、仮想パーティションを作成することができる。したがって、本明細書で使用される時に、パーティションは、メモリの物理的に区分された部分（物理パーティション）、メモリの論理的に区

10

20

30

40

50

分された部分（論理パーティション）、ならびに／または本明細書で説明される複数のアプリケーションにまたがって1もしくは複数のポリシおよび／もしくはポリシ・ファイルの実施の結果として作成される仮想パーティション（仮想パーティション）と呼ばれる場合がある。言い換えると、マネージド・アプリケーションに対してポリシを実施することによって、これらのアプリケーションは、他のマネージド・アプリケーションおよび信頼される企業リソースと通信できることに制限され、これによって管理されないアプリケーションおよびデバイスによって進入不可能な仮想パーティションを作成することができる。

【0054】

セキュア・アプリケーションは、電子メール・アプリケーション、ウェブ・ブラウジング・アプリケーション、ソフトウェアアズアサービス（SaaS）アクセス・アプリケーション、Windows（登録商標）Applicationアクセス・アプリケーション、および類似物とすることができる。セキュア・アプリケーションは、セキュア・ネイティブ・アプリケーション514、セキュア・アプリケーション・ランチャ518によって実行されるセキュア・リモート・アプリケーション522、セキュア・アプリケーション・ランチャ518によって実行される仮想化アプリケーション526、および類似物とすることができる。セキュア・ネイティブ・アプリケーション514は、セキュア・アプリケーション・ラッパー520によってラップされ得る。セキュア・アプリケーション・ラッパー520は、セキュア・ネイティブ・アプリケーション514がモバイル・デバイス502上で実行される時にモバイル・デバイス502上で実行される統合されたポリシを含むことができる。セキュア・アプリケーション・ラッパー520は、セキュア・ネイティブ・アプリケーション514の実行時に要求されるタスクを完了するためにセキュア・ネイティブ・アプリケーション514が要求する可能性がある企業でホスティングされるリソース（たとえば、504および508）に、モバイル・デバイス502上で走行するセキュア・ネイティブ・アプリケーション514を指すメタデータを含むことができる。セキュア・アプリケーション・ランチャ518によって実行されるセキュア・リモート・アプリケーション522は、セキュア・アプリケーション・ランチャ518内で実行され得る。セキュア・アプリケーション・ランチャ518によって実行される仮想化アプリケーション526は、モバイル・デバイス502上のリソース、企業リソース504、および類似物を利用することができる。セキュア・アプリケーション・ランチャ518によって実行される仮想化アプリケーション526によってモバイル・デバイス502上で使用されるリソースは、ユーザ対話リソース、処理リソース、および類似物を含むことができる。ユーザ対話リソースは、キーボード入力、マウス入力、カメラ入力、触覚入力、オーディオ入力、視覚入力、ジェスチャ入力、および類似物を収集し、送信するのに使用され得る。処理リソースは、ユーザ・インターフェースを提示し、企業リソース504から受信されたデータを処理し、類似物を行うのに使用され得る。セキュア・アプリケーション・ランチャ518によって実行される仮想化アプリケーション526によって企業リソース504で使用されるリソースは、ユーザ・インターフェース生成リソース、処理リソース、および類似物を含むことができる。ユーザ・インターフェース生成リソースは、ユーザ・インターフェースをアSEMBルし、ユーザ・インターフェースを変更し、ユーザ・インターフェースをリフレッシュし、類似物を行うのに使用され得る。処理リソースは、情報を作成し、情報を読み取り、情報を更新し、情報を削除し、類似物を行うのに使用され得る。たとえば、仮想化アプリケーション526は、グラフィカル・ユーザ・インターフェース（GUI）に関連するユーザ対話を記録し、これらをサーバ・アプリケーションに通信することができ、サーバ・アプリケーションは、サーバ上で動作するアプリケーションへの入力としてユーザ対話データを使用する。そのような配置では、企業は、サーバ側のアプリケーションならびにそのアプリケーションに関連するデータ、ファイル、その他を維持することを選択することができる。企業が、モバイル・デバイス502上での展開のために一部のアプリケーションを保護することによって本明細書の原理に従ってそれらのアプリケーションを「モバイル化」することを選択できるが、この配置は、ある

10

20

30

40

50

種のアプリケーションについても選択され得る。たとえば、一部のアプリケーションは、モバイル・デバイス502上での使用のために保護され得るが、他のアプリケーションは、モバイル・デバイス502での展開のために準備されず、またはそれに適切ではない可能性があり、したがって、企業は、仮想化技法を介して準備されていないアプリケーションへのモバイル・ユーザ・アクセスを提供することを選択することができる。別の例として、企業は、企業が仮想化技法を介してアプリケーションへのアクセスを提供することを選択できるようにモバイル・デバイス502用にアプリケーションをカスタマイズすることが非常に困難または他の形で望ましくない場合に、大きく不雑なデータ・セットを有する大きく複雑なアプリケーション（たとえば、材料リソース・プランニング・アプリケーション）を有する場合がある。もう1つの例として、企業は、企業がアプリケーションおよびデータへのモバイル・アクセスを許可するのに仮想化技法を使用することを選択できるように、保護されたモバイル環境に関してさえ機密性が高すぎると企業が見なす可能性がある高度に保護されたデータ（たとえば、人材データ、顧客データ、エンジニアリング・データ）を維持するアプリケーションを有する場合がある。企業は、モバイル・デバイス502上の十分に保護され十分に機能するアプリケーションとサーバ側でより正しく操作されると考えられるアプリケーションへのアクセスを可能にするための仮想化アプリケーション526との両方を提供することを選択することができる。一実施形態では、仮想化アプリケーション526は、モバイル・デバイス502上のセキュア・ストレージ位置のうちの1つに一部のデータ、ファイル、その他を記憶することができる。企業は、たとえば、他の情報を許可せずに、ある種の情報がモバイル・デバイス502上に記憶されることを許すことを選択することができる。

10

20

【0055】

本明細書で説明される仮想化アプリケーション526に関連して、モバイル・デバイス502は、GUIを提示し、その後にGUIとのユーザ対話を記録するように設計された仮想化アプリケーション526を有することができる。仮想化アプリケーション526は、アプリケーションとのユーザ対話としてサーバ側アプリケーションによって使用されるユーザ対話をサーバ側に通信することができる。これに応答して、サーバ側のアプリケーションは、新しいGUIをモバイル・デバイス502に送り返すことができる。たとえば、新しいGUIは、静的ページ、動的ページ、アニメーション、または類似物とし、これによって、リモートに配置されたリソースへのアクセスを提供することができる。

30

【0056】

セキュア・アプリケーション514は、モバイル・デバイス502の管理されるパーティション510内のセキュア・データ・コンテナ528内に記憶されたデータにアクセスすることができる。セキュア・データ・コンテナ内に保護されたデータは、セキュア・ネイティブ・アプリケーション514、セキュア・アプリケーション・ランチャ518によって実行されるセキュア・リモート・アプリケーション522、セキュア・アプリケーション・ランチャ518によって実行される仮想化アプリケーション526、および類似物によってアクセスされ得る。セキュア・データ・コンテナ528内に記憶されたデータは、ファイル、データベース、および類似物を含むことができる。セキュア・データ・コンテナ528内に記憶されたデータは、特定のセキュア・アプリケーション530に制限されたデータ、セキュア・アプリケーション532の間で共有されるデータ、および類似物を含むことができる。セキュア・アプリケーションに制限されたデータは、セキュア一般データ534および高度にセキュアなデータ538を含むことができる。セキュア一般データは、Advanced Encryption Standard (AES) 128ビット暗号化または類似物などの強い形の暗号化を使用することができ、高度にセキュアなデータ538は、AES 256ビット暗号化などの非常に強い形の暗号化を使用することができる。セキュア・データ・コンテナ528内に記憶されたデータは、デバイス・マネージャ524からのコマンドの受信時にモバイル・デバイス502から削除され得る。セキュア・アプリケーション（たとえば514、522、および526）は、二重モード・オプション540を有することができる。二重モード・オプション540は、ユーザ

40

50

に、保護されないモードまたは管理されないモードで保護されたアプリケーションを動作させるオプションを提示することができる。保護されないモードまたは管理されないモードでは、セキュア・アプリケーションは、モバイル・デバイス502の管理されないパーティション512上の保護されないデータ・コンテナ542内に記憶されたデータにアクセスすることができる。保護されないデータ・コンテナ内に記憶されたデータは、パーソナル・データ544とすることができる。保護されないデータ・コンテナ542内に記憶されたデータは、モバイル・デバイス502の管理されないパーティション512上で走行している保護されないアプリケーション546によってもアクセスされ得る。保護されないデータ・コンテナ542内に記憶されたデータは、セキュア・データ・コンテナ528内に記憶されたデータがモバイル・デバイス502から削除される時にモバイル・デバイス502上に留まることができる。企業は、ユーザによって所有され、ライセンス交付され、または制御されるパーソナル・データ、ファイル、および／またはアプリケーション（パーソナル・データ）を残しまたは他の形で保存しながら、企業によって所有され、ライセンス交付され、または制御される選択されたまたはすべてのデータ、ファイル、および／またはアプリケーション（企業データ）をモバイル・デバイス502から削除することを望む場合がある。この動作は、選択的ワイプと呼ばれる場合がある。企業データおよびパーソナル・データが本明細書で説明される態様に従って配置された状態で、企業は、選択的ワイプを実行することができる。

【0057】

モバイル・デバイス502は、企業の企業リソース504および企業サービス508に、公衆インターネット548に、および類似物に接続することができる。モバイル・デバイス502は、仮想プライベート・ネットワーク接続を介して企業リソース504および企業サービス508に接続することができる。仮想プライベート・ネットワーク接続は、microVPNまたはアプリケーション固有VPN(application-specific VPN)とも呼ばれるが、特定のアプリケーション550、特定のデバイス、モバイル・デバイス上の特定の保護された区域552、および類似物に固有とすることができる。たとえば、モバイル・デバイス502の保護された区域内のラップされたアプリケーションのそれぞれは、VPNへのアクセスが、おそらくはユーザまたはデバイスの属性情報に関連する、アプリケーションに関連する属性に基づいて許可されるように、アプリケーション固有VPNを介して企業リソースにアクセスすることができる。仮想プライベート・ネットワーク接続は、Microsoft Exchangeトラフィック、Microsoft Active Directoryトラフィック、ハイパーテキスト転送プロトコル(HTTP)トラフィック、HyperText Transfer Protocol Secure(HTTPS)トラフィック、アプリケーション管理トラフィック、および類似物を搬送することができる。仮想プライベート・ネットワーク接続は、シングルサインオン認証プロセス554をサポートし、使用可能にすることができる。シングルサインオン・プロセスは、ユーザが、認証サービス558によってその後を検証される認証証明書の単一のセットを提供することを可能にすることができる。認証サービス558は、ユーザが各個々の企業リソース504に認証証明書を提供することを要求せずに、複数の企業リソース504へのユーザ・アクセスを許可することができる。

【0058】

仮想プライベート・ネットワーク接続は、アクセス・ゲートウェイ560によって確立され、管理され得る。アクセス・ゲートウェイ560は、モバイル・デバイス502への企業リソース504の配送を管理し、加速し、改善する性能強化特徴を含むことができる。アクセス・ゲートウェイ560は、モバイル・デバイス502からのトラフィックを公衆インターネット548に再ルーティングし、モバイル・デバイス502が公衆インターネット548上で走行する公に使用可能な保護されていないアプリケーションにアクセスすることを可能にすることもできる。モバイル・デバイス502は、トランスポート・ネットワーク562を介してアクセス・ゲートウェイに接続することができる。トランスポート・ネットワーク562は、有線ネットワーク、無線ネットワーク、クラウド・ネット

10

20

30

40

50

ワーク、ローカル・エリア・ネットワーク、メトロポリタン・エリア・ネットワーク、広域ネットワーク、公衆ネットワーク、私有ネットワーク、および類似物とすることができる。

【0059】

企業リソース504は、電子メール・サーバ、ファイル共有サーバ、SaaSアプリケーション、ウェブ・アプリケーション・サーバ、Windows（登録商標）アプリケーション・サーバ、および類似物を含むことができる。電子メール・サーバは、Exchangeサーバ、Lotus Notesサーバ、および類似物を含むことができる。ファイル共有サーバは、ShareFileサーバおよび類似物を含むことができる。SaaSアプリケーションは、Salesforceおよび類似物を含むことができる。Windows（登録商標）アプリケーション・サーバは、ローカルWindows（登録商標）オペレーティング・システム上で走行することを意図されたアプリケーションおよび類似物を提供するように構築された任意のアプリケーション・サーバを含むことができる。企業リソース504は、構内ベースのリソース、クラウドベースのリソース、および類似物とすることができる。企業リソース504は、モバイル・デバイス502によって直接にまたはアクセス・ゲートウェイ560を介してアクセスされ得る。企業リソース504は、モバイル・デバイス502によってトランスポート・ネットワーク562を介してアクセスされ得る。

【0060】

企業サービス508は、認証サービス558、脅威検出サービス564、デバイス・マネージャ・サービス524、ファイル共有サービス568、ポリシ・マネージャ・サービス570、ソーシャル統合サービス572、アプリケーション・コントローラ・サービス574、および類似物を含むことができる。認証サービス558は、ユーザ認証サービス、デバイス認証サービス、アプリケーション認証サービス、データ認証サービス、および類似物を含むことができる。認証サービス558は、証明書を使用することができる。証明書は、モバイル・デバイス502上で、企業リソース504によって、および類似物によって記憶され得る。モバイル・デバイス502上に記憶された証明書は、モバイル・デバイス502上の暗号化された位置に記憶され得、証明書は、認証時の使用および類似物のためにモバイル・デバイス502上に一時的に記憶され得る。脅威検出サービス564は、進入検出サービス、不認可アクセス試行検出サービス、および類似物を含むことができる。不認可アクセス試行検出サービスは、デバイス、アプリケーション、データ、および類似物にアクセスする認可されていない試みを含むことができる。デバイス管理サービス524は、構成サービス、提供サービス、セキュリティ・サービス、サポート・サービス、監視サービス、報告サービス、およびデコミッションング・サービスを含むことができる。ファイル共有サービス568は、ファイル管理サービス、ファイル・ストレージ・サービス、ファイル・コラボレーション・サービス、および類似物を含むことができる。ポリシ・マネージャ・サービス570は、デバイス・ポリシ・マネージャ・サービス、アプリケーション・ポリシ・マネージャ・サービス、データ・ポリシ・マネージャ・サービス、および類似物を含むことができる。ソーシャル統合サービス572は、連絡先統合サービス、コラボレーション・サービス、Facebook、Twitter、およびLinkedInなどのソーシャル・ネットワークとの統合、ならびに類似物を含むことができる。アプリケーション・コントローラ・サービス574は、管理サービス、提供サービス、展開サービス、割当サービス、取消サービス、ラッピング・サービス、および類似物を含むことができる。

【0061】

企業モビリティ技術アーキテクチャ500は、アプリケーション・ストア578を含むことができる。アプリケーション・ストア578は、ラップ解除されたアプリケーション580、事前にラップされたアプリケーション582、および類似物を含むことができる。アプリケーションは、アプリケーション・コントローラ574からアプリケーション・ストア578に投入され得る。アプリケーション・ストア578は、アクセス・ゲートウ

10

20

30

40

50

エイ560を介して、公衆インターネット548を介して、または類似物を介してモバイル・デバイス502によってアクセスされ得る。アプリケーション・ストア578は、直観的で使い易いユーザ・インターフェースと共に提供され得る。

【0062】

ソフトウェア開発キット584は、この説明で前に説明したようにアプリケーションをラップすることによって、ユーザによって選択されたアプリケーションを保護する能力をユーザに与えることができる。ソフトウェア開発キット584を使用してラップされたアプリケーションは、アプリケーション・コントローラ574を使用してこれをアプリケーション・ストア578に投入することによって、モバイル・デバイス502から使用可能にされ得る。

10

【0063】

企業モビリティ技術アーキテクチャ500は、管理および解析能力588を含むことができる。管理および解析能力588は、リソースがどのように使用されるのか、リソースがどれほどしばしば使用されるのか、および類似物に関する情報を提供することができる。リソースは、デバイス、アプリケーション、データ、および類似物を含むことができる。リソースがどのように使用されるのかは、どのデバイスがどのアプリケーションをダウンロードするのか、どのアプリケーションがどのデータにアクセスするのか、および類似物を含むことができる。リソースがどれほどしばしば使用されるのかは、アプリケーションがどれほどしばしばダウンロードされたのか、データの特定のセットがアプリケーションによって何回アクセスされたのか、および類似物を含むことができる。

20

【0064】

図6は、別の例示的な企業モビリティ管理システム600である。上で図5を参照して説明されたモビリティ管理システム500の構成要素の一部は、単純さのために省略されている。図6に示されたシステム600のアーキテクチャは、上で図5を参照して説明したシステム500のアーキテクチャに多くの点で類似し、上で言及されなかった追加の特徴を含む可能性がある。

【0065】

この場合に、左側は、クライアント・エージェント604を有する登録されたモバイル・デバイス602を表し、クライアント・エージェント604は、右上に示されたExchange、SharePoint、公開鍵基盤(PKI)リソース、Kerberosリソース、証明書発行サービスなどの様々な企業リソース608および企業サービス609にアクセスするためにゲートウェイ・サーバ606(アクセス・ゲートウェイ機能性およびアプリケーション・コントローラ機能性を含む)と相互作用する。具体的に図示されていないが、モバイル・デバイス602は、アプリケーションの選択およびダウンロードのために企業アプリケーション・ストア(StoreFront)と相互作用することもできる。

30

【0066】

クライアント・エージェント604は、企業データ・センタ内でホスティングされるWindows(登録商標)アプリケーション/デスクトップのUI(ユーザ・インターフェース)媒介物として働き、このWindows(登録商標)アプリケーション/デスクトップは、High-Definition User Experience(HDX)/ICAディスプレイ・リモート処理プロトコルを使用してアクセスされる。クライアント・エージェント604は、ネイティブのiOSまたはAndroid(登録商標)のアプリケーションなど、モバイル・デバイス602上のネイティブ・アプリケーションのインストールおよび管理をもサポートする。たとえば、この図の上を示されたマネージド・アプリケーション610(メール、ブラウザ、ラップされたアプリケーション)は、すべて、モバイル・デバイス602上でローカルに実行するネイティブ・アプリケーションである。このアーキテクチャのクライアント・エージェント604およびアプリケーション管理フレームワークは、ポリシー駆動管理能力ならびに接続性およびSSO(シングル・サイン・オン)などの特徴を企業リソース/サービス608に提供するように働く。クラ

40

50

クライアント・エージェント 604 は、企業への、通常は他のゲートウェイ・サーバ構成要素への SSO を用いるゲートウェイ・サーバ 606 のアクセス・ゲートウェイ (AG) へのプライマリ・ユーザ認証を処理する。クライアント・エージェント 604 は、モバイル・デバイス 602 上のマネージド・アプリケーション 610 の挙動を制御するためにゲートウェイ・サーバ 606 からポリシを入手する。

【0067】

ネイティブ・アプリケーション 610 とクライアント・エージェント 604 との間のセキュア・プロセス間通信 (IPC) リンク 612 は、クライアント・エージェントが、アプリケーション管理フレームワーク 614 が各アプリケーションを「ラップする」ことによって実施されるポリシを供給することを可能にすることができる管理チャネルを表す。IPC チャンネル 612 は、クライアント・エージェント 604 が、企業リソース 608 への接続性および SSO を可能にする証明書および認証情報を供給することをも可能にすることができる。最後に、IPC チャンネル 612 は、アプリケーション管理フレームワーク 614 が、オンラインおよびオフラインの認証など、クライアント・エージェント 604 によって実施されるユーザ・インターフェース機能を呼び出すことを可能にすることができる。

10

【0068】

クライアント・エージェント 604 とゲートウェイ・サーバ 606 との間の通信は、本質的に、各ネイティブ・マネージド・アプリケーション 610 をラップするアプリケーション管理フレームワーク 614 からの管理チャネルの延長である。アプリケーション管理フレームワーク 614 は、クライアント・エージェント 604 にポリシ情報を要求することができる。クライアント・エージェント 604 は、これをゲートウェイ・サーバ 606 に要求することができる。アプリケーション管理フレームワーク 614 は、認証を要求することができる。クライアント・エージェント 604 は、ゲートウェイ・サーバ 606 のゲートウェイ・サービス部分 (NETSCALER ACCESS GATEWAY と称する) にログインすることができる。下でより十分に説明するように、クライアント・エージェント 604 は、ゲートウェイ・サーバ 606 上のサポートするサービスを呼び出すこともでき、ゲートウェイ・サーバ 606 は、ローカル・データ貯蔵室 616 の暗号化鍵を導出するための入力材料を作ることができ、あるいは、PKI 保護されたリソースへの直接認証を可能にするのできるクライアント証明書を提供することができる。

20

30

【0069】

より詳細には、アプリケーション管理フレームワーク 614 は、各マネージド・アプリケーション 610 を「ラップする」。これは、明示的なビルド・ステップを介して、またはビルド後の処理ステップを介して組み込まれ得る。アプリケーション管理フレームワーク 614 は、セキュア IPC チャンネル 612 を初期化し、アプリケーション 610 のポリシを入手するために、そのアプリケーションの初回起動時にクライアント・エージェント 604 と「対になる」ことができる。アプリケーション管理フレームワーク 614 は、クライアント・エージェント・ログイン依存性およびローカル OS サービスがどのように使用され得るのかまたはローカル OS サービスがどのようにマネージド・アプリケーション 610 と相互作用できるのかを制限する封じ込めポリシの一部など、ローカルに適用されるポリシの関連部分を実施することができる。

40

【0070】

アプリケーション管理フレームワーク 614 は、認証および内部ネットワーク・アクセスを容易にするために、セキュア IPC チャンネル 612 を介してクライアント・エージェント 604 によって提供されるサービスを使用することができる。私有および共有データ貯蔵室 616 (コンテナ) の鍵管理は、マネージド・アプリケーション 610 とクライアント・エージェント 604 との間の適当な相互作用によっても管理され得る。貯蔵室 616 は、オンライン認証の後でのみ使用可能とすることができ、あるいは、ポリシによって許可される場合には、オフライン認証の後に使用可能とすることができ、貯蔵室 616 の初回使用は、オンライン認証を要求することができ、オフライン・アクセスは、多くと

50

も、オンライン認証がもう一度要求される前のポリシ・リフレッシュ期間に制限され得る。

【0071】

内部リソースへのネットワーク・アクセスは、アクセス・ゲートウェイ606を介して個々のマネージド・アプリケーション610から直接に発生することができる。アプリケーション管理フレームワーク614は、各マネージド・アプリケーション610の代わりにネットワーク・アクセスを調整する責任を負うものとして行うことができる。クライアント・エージェント604は、オンライン認証の後に入手される適切な時間制限された副証明書を提供することによって、これらのネットワーク接続を容易にすることができる。リバー

10

【0072】

メールおよびブラウザ・マネージド・アプリケーション610は、特殊な状況を有し、任意のラップされたアプリケーションから一般に使用可能ではない可能性があるファシリティを利用することができる。たとえば、メール・アプリケーション610は、フルAGログオンを必要とせずに延長された時間期間にわたってExchangeサーバ608にアクセスすることを可能にする特殊なバックグラウンド・ネットワーク・アクセス機構を使用することができる。ブラウザ・アプリケーション610は、異なる種類のデータを分離するために複数の私有データ貯蔵室616を使用することができる。

20

【0073】

このアーキテクチャは、様々な他のセキュリティ特徴の組み込みをサポートすることができる。たとえば、いくつかの例のゲートウェイ・サーバ606（そのゲートウェイ・サービスを含む）は、アクティブ・ディレクトリ（AD）パスワードを妥当性検査する必要がある場合がある。ADパスワードが一部の状況で一部のユーザに関して認証要因として使用され得るかどうかは、企業の裁量に任され得る。ユーザがオンラインまたはオフライン（すなわち、ネットワークに接続されまたは未接続）である場合に、異なる認証方法が使用され得る。

【0074】

ステップ・アップ認証は、ゲートウェイ・サーバ606が、強い認証を要求する高度機密データへのアクセスを有することを許可されるマネージド・ネイティブ・アプリケーション610を識別し、これらのアプリケーションへのアクセスが、適当な認証を実行した後に限って許可される（これが、以前のより弱いレベルのログインの後に、再認証がユーザによって要求されることを意味する場合であっても）ことを確実にすることができる特徴である。

30

【0075】

この解決策の別のセキュリティ特徴は、モバイル・デバイス602上でのデータ貯蔵室616（コンテナ）の暗号化である。貯蔵室616は、ファイル、データベース、および構成を含むすべてのオンデバイス・データが保護されるようにするために暗号化され得る。オンライン貯蔵室に関して、鍵はサーバ（ゲートウェイ・サーバ606）上で記憶され得、オフライン貯蔵室に関して、鍵のローカル・コピーは、ユーザ・パスワードまたは生

40

【0076】

他のセキュア・コンテナも実施され得る。たとえば、マネージド・アプリケーション610の内部で発生するセキュリティ・イベントがログ記録され、バックエンドに報告される、ログ記録特徴を含めることができる。マネージド・アプリケーション610が改竄を検出する場合またはその時、ユーザ・データが破壊されたことのヒントをファイル・システム上に残さずに、関連する暗号化鍵がランダム・データによって上書きされ得るなど、データ・ワイピングがサポートされ得る。アプリケーションが、すべてのデータがスクリ

50

ーンショット内に記憶されることを防止できる、スクリーンショット保護を、もう1つの特徴とすることができる。たとえば、鍵ウィンドウの隠しプロパティにYESをセットすることができる。これは、現在スクリーン上に表示されているあらゆるコンテンツを隠し、通常はコンテンツが存在するはずの場所で黒いスクリーンショットをもたらすことができる。

【0077】

たとえばデータをコピーするか外部のアプリケーションに送ることによって、すべてのデータがアプリケーション・コンテナの外部にローカルに転送されるのを防止することによるなど、ローカル・データ転送が防止され得る。キーボード・キャッシュ特徴は、機密テキスト・フィールドのオートコレクト機能性を使用不能にするように動作することができる。SSL証明書妥当性検査は、アプリケーションが、キーチェーン内に記憶されるのではなくサーバSSL証明書を特に妥当性検査するように動作可能とすることができる。モバイル・デバイス602上でデータを暗号化するのに使用される鍵が、ユーザによって供給されるパスフレーズまたは生体測定データを使用して生成されるように、暗号化鍵生成特徴が使用され得る（オフライン・アクセスが要求される場合に）。オフライン・アクセスが要求されない場合には、鍵は、ランダムに生成された別の鍵と排他的論理和をとられ、サーバ側で記憶され得る。ユーザ・パスワードから生成される鍵が、その暗号ハッシュを作成するのではなく、KDF（鍵導出関数、特筆すべきはPassword-Based Key Derivation Function 2（PBKDF2））を使用するように、鍵導出関数が動作することができる。暗号ハッシュの作成は、鍵を、ブルート・フォース攻撃または辞書攻撃を許すものにする。

【0078】

さらに、1つまたは複数の初期化ベクトルが、暗号化方法で使用され得る。初期化ベクトルは、同一の暗号化されたデータの複数のコピーに、異なる暗号テキスト出力を作らせ、リプレイ・アタックと暗号解読攻撃との両方を防止する。これは、データを暗号化するのに使用される特定の初期化ベクトルが知られていない場合に、攻撃者が盗まれた暗号化鍵を用いてデータを暗号化解除することをも防止する。さらに、認証およびその後暗号化解除が使用され得、ここで、アプリケーション・データは、ユーザがアプリケーション内で認証された後に限って暗号化解除される。別の特徴は、メモリ内の機密データに関するものとしてことができ、この機密データは、必要な時に限ってメモリ内に（ディスク内ではなく）保持され得る。たとえば、ログイン証明書は、ログイン後にメモリからワイプされ得、暗号化鍵およびobjective-Ｃインスタンス変数内の他のデータは、簡単に参照され得るので記憶されない。その代わりに、メモリが、これらのために手動で割り振られ得る。

【0079】

ポリシーによって定義された非アクティブの期間の後に、ユーザ・セッションが打ち切られる、非アクティブ・タイムアウトが実施され得る。

【0080】

アプリケーション管理フレームワーク614からのデータ漏洩は、他の形で防止され得る。たとえば、マネージド・アプリケーション610がバックグラウンドに配置される場合またはその時に、メモリは、所定の（構成可能な）時間期間の後にクリアされ得る。バックグラウンド化される時に、フォアグラウンド化処理を高速化するためにアプリケーションの最後に表示されたスクリーンのスナップショットがとられ得る。スクリーンショットは、機密データを含む場合があり、したがってクリアされなければならない。

【0081】

もう1つのセキュリティ特徴は、1つまたは複数のアプリケーションへのアクセスのためのAD（アクティブ・ディレクトリ）622パスワードの使用を伴わないOTP（ワン・タイム・パスワード）620の使用に関するものとしてすることができる。いくつかの場合に、一部のユーザは、彼らのADパスワードを知らず（または知ることを許可されず）、したがって、これらのユーザは、SecurIDなどのハードウェアOTPシステムを使

10

20

30

40

50

用することによるなど、OTP 620を使用して認証することができる（OTPは、EntrustまたはGemaltoなどの異なるベンダによっても提供され得る）。いくつかの場合に、ユーザがユーザIDを用いて認証した後に、テキストが、OTP 620と共にユーザに送られ得る。いくつかの場合に、これは、オンライン使用のみに関して実施され得、プロンプトは単一のフィールドである。

【0082】

オフライン・パスワードは、オフライン使用が企業ポリシーを介して許可されるマネージド・アプリケーション610のオフライン認証に関して実施され得る。たとえば、企業は、StoreFrontがこの形でアクセスされることを望む場合がある。この場合に、クライアント・エージェント604は、ユーザがカスタム・オフライン・パスワードをセッ

10

【0083】

もう1つの特徴は、副証明書としてのある種のアプリケーション610に関するクライアント側証明書の使用可能化に関するものとして行うことができる（アプリケーション管理フレームワークmicroVPN特徴を介してPKI保護されたウェブ・リソースにアクセスするための）。たとえば、マネージド・アプリケーション610は、そのような証明書を利用することができる。この場合に、ActiveSyncプロトコルを使用する証明書ベースの認証がサポートされ得、ここで、クライアント・エージェント604からの証明書は、ゲートウェイ・サーバ606によって取り出され、キーチェーン内で使用され得る。各マネージド・アプリケーション610は、ゲートウェイ・サーバ606内で定義されるラベルによって識別される、1つの関連するクライアント証明書を有することができる。

20

【0084】

ゲートウェイ・サーバ606は、関連するマネージド・アプリケーションが内部PKI保護されたリソースに認証することを可能にするためのクライアント証明書の発行をサポートするために、企業特殊目的ウェブ・サービスと相互作用することができる。

30

【0085】

クライアント・エージェント604およびアプリケーション管理フレームワーク614は、内部PKI保護されたネットワーク・リソースへの認証のためのクライアント証明書の入手および使用をサポートするように機能強化され得る。様々なレベルのセキュリティ要件および／または分離要件と一致するためなど、複数の証明書がサポートされ得る。証明書は、メールおよびブラウザ・マネージド・アプリケーション610によって、ならびに最終的には任意のラップされたアプリケーション610によって使用され得る（アプリケーション管理フレームワークがHTTPS要求を仲裁することが穏当である場合に、これらのアプリケーションが、ウェブ・サービス・スタイルの通信パターンを使用すると仮定して）。

40

【0086】

iOS上でのアプリケーション管理クライアント証明書サポートは、使用の期間ごとに各マネージド・アプリケーション610内のiOSキーチェーンにpublic-key cryptography standards (PKCS) 12 BLOB（バイナリ・ラージ・オブジェクト）をインポートすることに頼ることができる。アプリケーション管理フレームワーク・クライアント証明書サポートは、私有メモリ内鍵ストレージを有するHTTPS実施態様を使用することができる。クライアント証明書は、iOSキーチェーン内に存在しないものとして行うことができ、潜在的に、強く保護される「オンライン専用」データ値内を除いて永続化されないものとして行うことができる。

【0087】

50

相互SSLも、モバイル・デバイス602が企業に認証され、その逆が行われることを要求することによって追加のセキュリティを提供するために実施され得る。ゲートウェイ・サーバ606への認証のための仮想スマート・カードも実施され得る。

【0088】

制限されたKerberosサポートとフルKerberosサポートとの両方が、追加の特徴とされ得る。フル・サポート特徴は、ADパスワードまたは信頼されるクライアント証明書を使用してアクティブ・ディレクトリ(AD)622へのフルKerberosログインを行い、HTTP Negotiate authenticationチャレンジに応答するためにKerberosサービス・チケットを入手する能力に関する。制限されたサポート特徴は、Citrix Access Gateway Enterprise Edition(AGEE)が、HTTP Negotiate authenticationチャレンジに応答してKerberosサービス・チケット(constrained delegationの対象)を入手し、使用できるように、Kerberosプロトコル遷移の呼出しをサポートする、AGEEでのconstrained delegationに関する。この機構は、リバース・ウェブ・プロキシ(別名、corporate virtual private network(CVPN))モードで、HTTP(HTTP/HTTPSではなく)接続がVPNモードおよびmicroVPNモードでプロキシ化される時に働く。

【0089】

もう1つの特徴は、脱獄(制限の非正規解除)またはルート化の検出時に自動的に発生でき、管理コンソールからプッシュされるコマンドとして発生し、マネージド・アプリケーション610が走行していない時であってもリモート・ワイプ機能性を含むことができる、アプリケーション・コンテナのロックおよびワイプに関するものとして行うことができる。

【0090】

ユーザが障害の場合に複数の異なる位置のうちの1つからサービスされることを可能にする、企業アプリケーション・ストアおよびアプリケーション・コントローラのマルチサイト・アーキテクチャまたはマルチサイト構成がサポートされ得る。

【0091】

いくつかの場合に、マネージド・アプリケーション610は、API(たとえば、OpenSSL)を介して証明書および秘密鍵にアクセスすることを可能にされ得る。企業の信頼されるマネージド・アプリケーション610は、アプリケーションのクライアント証明書および秘密鍵を用いて特定の公開鍵動作を実行することを可能にされ得る。アプリケーションがブラウザのように振る舞い、証明書アクセスが要求されない場合またはその時、アプリケーションが「私は誰か」に関して証明書を読み取る場合またはその時、アプリケーションがセキュア・セッション・トークンを構築するために証明書を使用する場合またはその時、アプリケーションが重要なデータ(たとえば、トランザクション・ログ)のデジタル署名のためまたは一時的なデータ暗号化のために秘密鍵を使用する場合またはその時など、様々なユース・ケースが識別され、それに応じて処理され得る。

【0092】

企業モビリティ管理アーキテクチャおよびピアツーピア通信

上で議論したように、モバイル・デバイスは、企業モビリティ技術アーキテクチャおよび/または企業モビリティ管理システムの諸態様を用いて構成される場合に、ユーザが企業リソース、企業サービス、および類似物にアクセスする能力を使用可能にすることができる。アクセスは、アクセス・ゲートウェイを用いて確立され、アクセス・ゲートウェイによって管理される複数の仮想プライベート・ネットワーク接続に基づくものとして行うことができる。しばしば、ユーザは、複数のデバイスを有する場合があり、企業技術アーキテクチャおよび/または企業モビリティ管理システムの諸態様を用いてそれぞれが構成される時に、デバイスのそれぞれは、ユーザが企業リソース、企業サービス、およびアクセス・ゲートウェイを介してアクセス可能な任意の他のサービス/リソースにアクセスする能

10

20

30

40

50

力を使用可能にすることができる。これらのデバイス（たとえば、タブレット、携帯電話機、他のコンピューティング・デバイス）のそれぞれは、異なる能力を有する可能性があり、これらの能力は、ユーザがアクセス・ゲートウェイを介してリソースおよびサービスにアクセスするのに各デバイスを使用できる形を変化させる場合がある。

【0093】

たとえば、1つのデバイスを、無線ネットワーク（たとえば、第3世代（3G）無線ネットワーク、第4世代（4G）無線ネットワーク、Long-Term Evolution（LTE）無線ネットワーク、WIFI無線ローカル・エリア・ネットワーク）に接続された携帯電話機とすることができ、無線ネットワークへの接続を介して、携帯電話機は、アクセス・ゲートウェイへの仮想プライベート・ネットワーク接続を確立できる場合がある。第2のデバイスを、無線ネットワークへの接続を有しないか、他の形でアクセス・ゲートウェイへの仮想プライベート・ネットワーク接続を確立することができないタブレット・コンピュータとすることができる。タブレット・コンピュータの、アクセス・ゲートウェイへの仮想プライベート・ネットワーク接続を確立する能力のなさは、企業モビリティ管理システムの潜在力を最大限まで使用する、ユーザの能力を減少させる。したがって、企業モビリティ管理システムに関するユーザの経験は、各デバイスのネットワーク接続性の相違にかかわらず、アクセス・ゲートウェイを介してリソースおよびサービスにアクセスするのに両方のデバイスを使用する能力をユーザが有する場合に改善され得る。これらの利益および他の利益は、下の議論および全体としての本開示に鑑みて明白である。具体的には、図7～図12および対応する説明は、とりわけ、アクセス・ゲートウェイを介して企業リソースおよび企業サービスにアクセスするのに複数のデバイスを使用可能にし、使用する例を提供する。

【0094】

図7は、ユーザが本明細書で説明される様々な態様に従って複数のデバイスを使用して企業リソースおよび企業サービスにアクセスできる可能性がある1つの例の配置を示す。例の配置は、3つのモバイル・デバイス702-A、702-B、および702-Cを含む。3つのモバイル・デバイスは、第1の位置701（たとえば、単一の家または構内、自動車、お互いからしきい距離内、特定のサイズの地理的区域、同一のセルラ塔によってサービスされる位置など）に配置されて図示されている。各デバイスは、図5に関連して説明した企業モビリティ技術アーキテクチャの諸態様を用いて構成され得（たとえば、モバイル・デバイス502と同様に構成される）、かつ／または図6に関連して説明した企業モビリティ管理システムの諸態様を用いて構成され得る（たとえば、モバイル・デバイス602と同様に構成される）。3つのモバイル・デバイス702-A、702-B、および702-Cのそれぞれは、同一のユーザ（図示せず）に関連付けられ得る。図7に示されたモバイル・デバイスの個数は、例示のためのものである。ユーザは、より多数またはより少数のモバイル・デバイスに関連付けられ得、本明細書で説明される方法は、異なる個数のモバイル・デバイスを有する配置にあてはまる。

【0095】

ユーザは、様々な企業リソース719および／または企業サービス717にアクセスし、使用するのに3つのモバイル・デバイス702-A、702-B、および702-Cのそれぞれを使用するつもりである場合がある。企業リソース719および企業サービス717へのアクセスおよびその使用は、アクセス・ゲートウェイ707によって管理され得る。アクセス・ゲートウェイ707、企業リソース719、および／または企業サービス717は、第1の位置701とは異なるまたはこれからリモートである第2の位置711に配置されたものとして図示されている。第2の位置711は、単純さのために図示されている。いくつかの配置では、企業リソース719、企業サービス719、およびアクセス・ゲートウェイ707は、お互いとは異なる位置に配置され得る。アクセス・ゲートウェイ707は、図5に関連して説明した企業モビリティ技術アーキテクチャの諸態様を用いて構成され得（たとえば、アクセス・ゲートウェイ560と同様に構成される）、かつ／または図6に関連して説明した企業モビリティ管理システムの諸態様を用いて構成され

得る（たとえば、ゲートウェイ・サーバ606と同様に構成される）。企業リソース719および企業リソースは、図5および図6に関連して議論したものに類似するものとすることができる（たとえば、企業リソース504、企業サービス508、企業リソース／サービス608、609、620、622、および類似物）。アクセス・ゲートウェイ707は、企業リソース719および企業サービス717に加えて、たとえば公衆インターネット548、アプリケーション・ストア578、および類似物へのアクセスを含む機能性を提供することもできる。

【0096】

3つのモバイル・デバイス702-A、702-B、および702-Cのそれぞれは、お互いとは異なる能力を有することができ、第1の位置701で使用可能なネットワークに基づいて、あるデバイスが、アクセス・ゲートウェイ707への仮想プライベート・ネットワーク接続を確立できない場合がある。図7に示されているように、モバイル・デバイス702-Cは、アクセス・ゲートウェイ707との仮想プライベート・ネットワーク接続713を確立済みである。やはり図7に示されているように、モバイル・デバイス702-Aおよび702-Bは、アクセス・ゲートウェイ707との仮想プライベート・ネットワーク接続を有しない。たとえば、モバイル・デバイス702-Cは、モバイル・デバイス702-Cがアクセス・ゲートウェイ707と通信することを可能にする無線ネットワーク709（たとえば、3G無線ネットワーク、4G無線ネットワーク、WIFI無線ローカル・エリア・ネットワーク、および類似物）に接続できるデバイスとすることができる。モバイル・デバイス702-Aおよび702-Bは、それぞれ、無線ネットワーク709に接続できないデバイス（たとえば、3G、4G、またはLTE無線ネットワークに接続する能力のないタブレット・コンピュータ）とすることができ、あるいは、ユーザが無線ネットワーク709に接続しないことを選択したデバイス（たとえば、機内モードにセットされたデバイスなど、使用不能にされた無線通信機を有するデバイス）とすることができる。

【0097】

仮想プライベート・ネットワーク接続713は、図5および図6に関連して議論したものと同様の、1つまたは複数のmicroVPN接続またはアプリケーション固有VPN接続とすることができる。そのような配置では、仮想プライベート・ネットワーク接続713は、アクセス・ゲートウェイ707と、たとえばモバイル・デバイス702-Cの1つまたは複数のマネージド・アプリケーション（たとえば、マネージド・アプリケーション514）および／またはモバイル・デバイス702-Cのクライアント・エージェント（たとえば、クライアント・エージェント604）を含む、モバイル・デバイス702-Cのモビリティ管理システムの様々な構成要素との間でのデータ・トラフィックの交換を可能にすることができる。仮想プライベート・ネットワーク接続713は、無線ネットワーク709（および、図7に明示的には図示されていない1つまたは複数の他のネットワーク）を通るトンネルとして働くことができる。仮想プライベート・ネットワーク接続713を介するデータの交換に適するマネージド・アプリケーションおよび／またはクライアント・エージェントのタイプのいくつかの例は、たとえば、Citrix System, Inc. によるアプリケーションのWORX suite（たとえば、Citrix Systems, Inc. によるWORX HOME、Citrix Systems, Inc. によるWORXMAILなど）、およびCitrix Systems, Inc. によるXENMOBILEと互換の他のアプリケーション／クライアント・エージェントを含む。

【0098】

3つのモバイル・デバイス702-A、702-B、および702-Cは、メッシュ・ネットワークのメンバ（またはノード）として構成され得る。メッシュ・ネットワークは、一般に、メンバがメッシュ・ネットワークの他のメンバにデータを中継するネットワークである。各メンバは、たとえばフラッディング技法またはルーティング技法を使用してデータを中継することができる。ルーティング技法が使用され得るが、明瞭さおよび議論

10

20

30

40

50

のしやすさのために、本開示は、ルーティング技法を使用するメッシュ・ネットワークの例を提供する。ルーティング技法の下では、データは、その最終宛先に達するまで、メンバからメンバへの一連のホップとしてメッシュ・ネットワーク全体にルーティングされ得る。したがって、図7に示されているように、モバイル・デバイス702-A、702-B、および702-Cは、メッシュ・ネットワークのメンバであり、データは、ピアツーピア接続703および705を介してメッシュ・ネットワーク全体にルーティングされ得る。ピアツーピア接続703および705は、たとえばBLUETOOTH（登録商標）プロトコル、WIFI DIRECTプロトコル、または物理的に非常に近接したデバイスの間の直接通信を可能にする任意の他のプロトコルを含む、様々なトランスポート・プロトコルを使用することができる。ピアツーピア接続703が、ピアツーピア接続705とは異なるトランスポート・プロトコルを使用することもできる。たとえば、ピアツーピア接続703が、BLUETOOTH（登録商標）プロトコルを使用することができ、ピアツーピア接続705が、WIFI DIRECTプロトコルを使用することができる。

10

【0099】

いくつかの配置で、ピアツーピア接続は、ピアツーピア接続を介して送信されるデータが暗号化されるようにするために、特定の暗号化方式を使用するように構成される。各ピアツーピア接続が、それ自体の暗号化方式を使用することができ（たとえば、ピアツーピア接続703を介して送信されるデータは、ピアツーピア接続705を介してデータを送信するのに使用される鍵とは異なる暗号化鍵を使用して暗号化される）、ピアツーピア接続の各タイプが、それ自体の暗号化方式を使用することができ（たとえば、BLUETOOTH（登録商標）接続を介して送信されるデータは、WIFI DIRECT接続を介して送信されるデータを暗号化するのに使用される鍵とは異なる暗号化鍵を使用して暗号化される）、あるいは、メッシュ・ネットワークが、単一の共通の暗号化方式を使用することができる（たとえば、同一の暗号化鍵／暗号化解除鍵が、各ピアツーピア接続を介して送信されるデータを暗号化し／暗号化解除するのに使用される）。暗号化方式は、企業管理フレームワークによって実施されるポリシー内で指定され得る。さらに、暗号化方式は、セキュア・コンテナまたはセキュア・データ貯蔵室内にデータを記憶するのに使用されるものと同一とすることができる（たとえば、セキュア・コンテナ528および／またはデータ貯蔵室616内に記憶されるデータを暗号化し／暗号化解除するのに使用される暗号化鍵／暗号化解除鍵が、ピアツーピア接続を介して送信されるデータを暗号化し／暗号化解除するために使用され得る）。

20

30

【0100】

さらに、モバイル・デバイス702-A、702-B、および702-Cの間に追加のピアツーピア接続がある場合がある。たとえば、ピアツーピア接続（図示せず）が、モバイル・デバイス702-Aとモバイル・デバイス702-Cとの間で確立され得る。別の例として、図示されたピアツーピア接続705に加えて、第2のピアツーピア接続（図示せず）が、モバイル・デバイス702-Aとモバイル・デバイス702-Bとの間で確立され得る。メッシュ・ネットワークの使用は、例示のためのものである。他のタイプのアドホック・ネットワークまたはピアツーピア・ネットワークが、本明細書で説明される諸態様を組み込んだ様々な実施形態内で使用され得る。メッシュ・ネットワークのメンバになるために各モバイル・デバイス702-A、702-B、および702-Cによって使用され得る例の方法が、下で図8に関連して議論される。メッシュ・ネットワークの確立に関するさらなる詳細は、図12に関連して議論される。

40

【0101】

図示の配置は、モバイル・デバイス702-Aおよび702-Bからのデータがアクセス・ゲートウェイ707によって受信されることを可能にすることができる。この形で、モバイル・デバイス702-Aおよび702-Bは、企業リソース719および企業サービス717を含む、アクセス・ゲートウェイ707によって制御され、かつ／または管理される機能性にアクセスし、かつ／または使用できる可能性がある。たとえば、アクセス

50

・ゲートウェイ707用のデータ（たとえば、モバイル・デバイス702-Aおよび702-Bのマネージド・アプリケーションまたはクライアント・エージェントによって生成されたデータ）は、メッシュ・ネットワークの1つまたは複数のピアツーピア接続703および/または705を介してモバイル・デバイス702-Cにルーティングされ、送信され得る。モバイル・デバイス702-Cによって受信された後に、データは、仮想プライベート・ネットワーク接続713を介してアクセス・ゲートウェイ707に送信され得る。同様に、アクセス・ゲートウェイ707は、モバイル・デバイス702-Aまたは702-B用のデータ（たとえば、企業リソース719または企業サービス717のアクセスに基づいて生成されたデータ）を、仮想プライベート・ネットワーク接続713を介してモバイル・デバイス702-Cに送信することができる。モバイル・デバイス702-Cによって受信された後に、データは、メッシュ・ネットワークの1つまたは複数のピアツーピア接続703および/または705を介して所期の宛先にルーティングされ、送信され得る。受信時に、モバイル・デバイス702-Aまたは702-Bは、アプリケーション管理フレームワークに従ってデータを処理することができる（たとえば、マネージド・アプリケーションにデータを供給する、データをコンテナ内に記憶するなど）。たとえば、モバイル・デバイス702-Bのマネージド・メール・アプリケーションは、ユーザが仮想プライベート・ネットワーク接続713を使用して新しい電子メールを受信することを可能にするために、アクセス・ゲートウェイ707を介して電子メール・データを受信することができる。別の例として、モバイル・デバイス702-Aのマネージド・ブラウザ・アプリケーションは、ユーザが仮想プライベート・ネットワーク接続713を使用してモバイル・デバイス702-Aからインターネットをブラウズすることを可能にするために、アクセス・ゲートウェイからウェブ・ブラウジング・データを受信できる可能性がある。さらに、メッシュ・ネットワークは、モバイル・デバイス702-A、702-B、および702-Cがアプリケーション管理フレームワークに関する様々な機能を実行することを可能にするのできるデータをこれらのモバイル・デバイスの間で送信するのに使用され得る。たとえば、ユーザがモバイル・デバイス702-A、702-B、および702-Cのうちの1つからのスクリーンを共有することを可能にするために、スクリーン共有データがこれらのデバイスの間で送信され得る。別の例として、ユーザがモバイル・デバイス702-A、702-B、および702-Cの間で電子メール・メッセージを同期化することを可能にするために、電子メール・データが、モバイル・デバイス702-A、702-B、および702-Cの間で送信され得る。メッシュ・ネットワークが企業モビリティ管理システムに関連してどのように使用され得るのかに関するさらなる詳細は、図11A～図11Dおよび図12に関連して議論される。

【0102】

図8は、メッシュ・ネットワークの確立に関連して使用され得る例の方法を示す。具体的には、図8の例の方法は、メッシュ・ネットワークのメンバになるか他の形でメッシュ・ネットワークを確立するのに図7のモバイル・デバイス702-A、702-B、および702-Cのそれぞれによって使用され得る。いくつかの配置では、図8のステップは、たとえば図6のクライアント・エージェント604を含む企業モビリティ管理システムの1つまたは複数の構成要素によって実行され得る。さらに、モバイル・デバイスは、メッシュ・ネットワークの確立を容易にするために、モバイル・デバイスの存在および近くのデバイスの発見をアドバタイズするのを援助するためにOPENGARDEN SDKなどの既存技術の変形形態を使用することができる。

【0103】

ステップ801では、モバイル・デバイスが、モバイル・デバイスがメッシュ・ネットワークに加わることを認可する指示を受信することができる。いくつかの配置では、指示は、メッシュ・ネットワークの確立を開始するか、他の形でモバイル・デバイスにメッシュ・ネットワークの確立を試みさせる、モバイル・デバイスとのユーザの対話に基づいて受信され得る。たとえば、モバイル・デバイスのユーザは、モバイル・デバイスの管理されるパーティション上に記憶されるメッシュ・ネットワーク・セッティングをトグルする

ことによって、メッシュ・ネットワークのメンバシップを認可することができる。別の例として、ユーザは、モビリティ管理システムのオプションのメニューを提供するユーザ・インターフェースを見ることができる場合がある。オプションの1つが、モバイル・デバイスがメッシュ・ネットワークのメンバになることを認可するためにユーザによってセットされ得る。いくつかの配置で、モバイル・デバイスは、ユーザにユーザ情報を要求することができる。たとえば、ユーザは、メッシュ・ネットワークのメンバシップを認証するためのユーザ情報として使用される1つまたは複数のセキュリティ証明書（たとえば、ユーザ名／パスワード、証明書、セキュアPINコードなど）を識別するように要求され得る。これに応答して、ユーザは、メッシュ・ネットワークのメンバシップを認証する時にモバイル・デバイスが使用すべき1つまたは複数のセキュリティ証明書を入力しまたは他の形で選択することができる。モバイル・デバイスがメッシュ・ネットワークに加わることを認可する指示を受信し、かつ／またはユーザ情報の識別を受信した後に、モバイル・デバイスは、ステップ803に進むことができる。

10

【0104】

ステップ803では、モバイル・デバイスが、モバイル・デバイスの1つまたは複数のアドバタイズメントを送信することができる。アドバタイズメントは、アドバタイズメントを受信できる他のデバイスにモバイル・デバイスの存在を示すことができ、トランスポート・プロトコルに固有とすることができる。たとえば、モバイル・デバイスは、たとえばBLUETOOTH（登録商標）およびWIFI DIRECTを含むピアツーピア通信が可能な複数のラジオを伴って構成され得る。したがって、モバイル・デバイスは、どのピアツーピア・ラジオまたはピアツーピア機能性がモバイル・デバイス上で現在アクティブであるのかに基づいて（たとえば、BLUETOOTH（登録商標）ラジオがアクティブであるかどうかを判定し、かつ／またはWIFI DIRECT機能性が使用可能にされているかどうかを判定する）、モバイル・デバイスがどのタイプのピアツーピア接続を確立できるのかを判定することができる。モバイル・デバイスが確立できるピアツーピア接続のタイプごとに、モバイル・デバイスは、ピアツーピア接続のそのタイプに対応するトランスポート・プロトコルを使用してアドバタイズメントを送信することができる。したがって、モバイル・デバイスは、BLUETOOTH（登録商標）通信を介して、BLUETOOTH（登録商標）プロトコルを使用してアドバタイズメントを送信することができる。モバイル・デバイスは、WIFI DIRECT通信を介して、WIFI DIRECTプロトコルを使用してアドバタイズメントを送信することができる。いくつかの配置では、ステップ803で送信される各アドバタイズメントは、ステップ801で識別されたセキュリティ証明書など、モバイル・デバイスのユーザ情報を含むことができる。

20

30

【0105】

ステップ805では、モバイル・デバイスが、1つまたは複数の他のモバイル・デバイスの1つまたは複数のアドバタイズメントを受信することができる。1つまたは複数の他のモバイル・デバイスのアドバタイズメントは、モバイル・デバイスに他のモバイル・デバイスの存在を示すことができ、トランスポート・プロトコルに固有とすることができる。さらに、1つまたは複数の他のデバイスの1つまたは複数のアドバタイズメントは、ステップ803に関連して議論したピアツーピア通信の同一のタイプを介して受信され得る（たとえば、ステップ805で受信されるアドバタイズメントのそれぞれは、BLUETOOTH（登録商標）通信を介するものおよび／またはWIFI DIRECT通信を介するものとしてすることができる）。いくつかの場合に、ステップ805で受信されるアドバタイズメントは、ステップ803でモバイル・デバイスによって送信されたアドバタイズメントに対する応答として他のモバイル・デバイスによって送信されたものである場合がある。たとえば、アドバタイズメントが、ステップ803でBLUETOOTH（登録商標）通信を介して送信された場合に、モバイル・デバイス（たとえば、モバイル・デバイス702-C）は、BLUETOOTH（登録商標）通信を介して、そのアドバタイズメントに対する応答として別のモバイル・デバイス（たとえば、モバイル・デバイス702

40

50

ーB)の少なくとも1つのアドバタイズメントを受信することができる。いくつかの配置では、ステップ805で受信される1つまたは複数のアドバタイズメントは、1つまたは複数の他のモバイル・デバイスのユーザ情報を含むことができる(たとえば、モバイル・デバイス702-Bのアドバタイズメントは、モバイル・デバイス702-Bのユーザによって選択されたセキュリティ証明書を含むことができる)。

【0106】

いくつかの例で、モバイル・デバイスは、モバイル・デバイスがタイムアウト期間(たとえば、10秒)以内に他のモバイル・デバイスからアドバタイズメントを全く受信できない場合に、メッシュ・ネットワークに加わる試みを使用不能にするように構成され得る。たとえば、ステップ803の1つまたは複数のアドバタイズメントの送信の後に、モバイル・デバイスは、他のモバイル・デバイスからのアドバタイズメントを待ち始めることができる。モバイル・デバイスが、タイムアウト期間内に他のモバイル・デバイスからのアドバタイズメントを全く受信できない場合に、モバイル・デバイスは、メッシュ・ネットワークを形成するための近くのデバイスがないことを示すエラー・メッセージをユーザに供給することができ、その後、この方法は終了する。

【0107】

ステップ807では、モバイル・デバイスが、ステップ805で受信した1つまたは複数のアドバタイズメントに基づいて、1つまたは複数の他のモバイル・デバイスのユーザ情報を判定することができる。たとえば、いくつかの配置では、各アドバタイズメントが、ユーザ情報を含むことができる。したがって、モバイル・デバイスは、ステップ805で受信したアドバタイズメントからユーザ情報を抽出することができる。他の配置では、ユーザ情報が、1つまたは複数のユーザ・デバイスに要求される必要がある場合がある。したがって、モバイル・デバイスは、ステップ805で受信したアドバタイズメントごとに、どのデバイスがそのアドバタイズメントを送信したのかを判定することができ、アドバタイズメントを送信したと判定された各デバイスに、ピアツーピア通信を介してユーザ情報要求を送信することができる。ユーザ情報要求を送信する際に、モバイル・デバイスは、ユーザ情報の受信を待つことができる。1つまたは複数の他のモバイル・デバイスのそれぞれのユーザ情報が判定された後に、この方法は、ステップ809に進むことができる。

【0108】

ステップ809では、モバイル・デバイスが、メッシュ・ネットワークのメンバシップを認証すべきかどうかを判定することができる。いくつかの配置では、この認証は、1つまたは複数の他のデバイスのユーザ情報およびモバイル・デバイスのユーザ情報に基づくものとすることができる。たとえば、モバイル・デバイスは、1つまたは複数の他のモバイル・デバイスごとに、モバイル・デバイスのユーザ情報(たとえば、ステップ801でユーザによって識別された1つまたは複数のセキュリティ証明書)が他のデバイスから受信したユーザ情報と一致するかどうかを判定することができる。他のデバイスのうちの少なくとも1つが、モバイル・デバイスのユーザ情報と一致するユーザ情報を有する場合には、モバイル・デバイスは、メッシュ・ネットワークのメンバシップが認証されると判定することができる。

【0109】

いくつかの配置で、モバイル・デバイスは、モバイル・デバイスおよび一致するユーザ情報を有する1つまたは複数のモバイル・デバイスに基づいて、メッシュ・ネットワークのメンバシップを認証することができる。言い換えると、メッシュ・ネットワークは、一致するユーザ情報を有するデバイスを含むように確立される。一致しないユーザ情報を提供するすべてのデバイスは、メッシュ・ネットワークのメンバシップを拒否される。たとえば、図7のモバイル・デバイスを例示的な例として使用すると、モバイル・デバイス702-Cは、2つのデバイスからのユーザ情報すなわち、モバイル・デバイス702-Aからのユーザ情報およびモバイル・デバイス702-Bからのユーザ情報を受信済みであるものとすることができる。この例では、モバイル・デバイス702-Cは、モバイル・

10

20

30

40

50

デバイス702-Aからのユーザ情報が一致するが、モバイル・デバイス702-Bからのユーザ情報が一致しないと判定することができる。この例では、モバイル・デバイス702-Cは、モバイル・デバイス702-Cおよびモバイル・デバイス702-Aだけを含むメッシュ・ネットワークのメンバシップを認証すると判定することができる。この例では、モバイル・デバイス702-Bは、メッシュ・ネットワークのメンバにならない。

【0110】

いくつかの変形形態では、モバイル・デバイスは、アクセス・ゲートウェイによって記憶された情報またはアクセス・ゲートウェイを介してアクセス可能である情報に基づいて、メッシュ・ネットワークのメンバシップを認証することができる。たとえば、アクセス・ゲートウェイ（またはアクセス・ゲートウェイを介してアクセス可能なサーバ）は、登録されたデバイスの識別情報を記憶することができる（たとえば、XENMOBILE SERVER（XMS）データベース内に）。いくつかの実施形態では、識別情報は、各登録されたデバイスがメッシュ・ネットワークに加わることを認可されるかどうかを指定することができ、かつ／またはユーザの識別を含むことができる。モバイル・デバイスは、仮想プライベート・ネットワーク・トンネルを介してアクセス・ゲートウェイにユーザ情報を送信することができる。アクセス・ゲートウェイを介する受信の後に、ユーザ情報と登録されたデバイスの識別情報との間で比較が実行され得る。この比較に基づいて、アクセス・ゲートウェイは、デバイスのそれぞれがメッシュ・ネットワークに加わることを許されるかどうかに関する指示を応答することができる。メッシュ・ネットワークに加わることを許されるすべてのデバイスは、メンバシップに関して認証され得る。メッシュ・ネットワークに加わることを許されないすべてのデバイスは、メンバシップを否定され得る。

【0111】

メッシュ・ネットワークのメンバシップを認証すると判定する時に、この方法は、ステップ811に進むことができる。モバイル・デバイスが、メッシュ・ネットワークのメンバシップを認証しないと判定する（たとえば、他のモバイル・デバイスのユーザ情報のいずれもが、モバイル・デバイスのユーザ情報と一致しない）場合には、この方法は終了する。

【0112】

ステップ811では、モバイル・デバイスが、1つまたは複数の他のモバイル・デバイスのうちの少なくとも1つにデータをルーティングするのに使用可能なルーティング情報を判定することができる。たとえば、モバイル・デバイスは、1つまたは複数の他のデバイスのどれが次のホップになるべきかを判定することができる。その後、モバイル・デバイスは、次のホップにデータを通信するためのルーティング情報を判定することができる。一特定の例では、メッシュ・ネットワークが図7の3つのモバイル・デバイスを含み、メッシュ・ネットワークが図7に示されたピアツーピア接続を使用して接続される場合に、モバイル・デバイス702-Bは、モバイル・デバイス702-Aおよび702-Bにデータを通信するためのルーティング情報を判定することができ、モバイル・デバイス702-Cは、モバイル・デバイス702-Bにデータを通信するためのルーティング情報を判定することができ、モバイル・デバイス702-Aは、モバイル・デバイス702-Bにデータを通信するためのルーティング情報を判定することができる。ルーティング情報を判定した時に、この方法はステップ813に進むことができる。

【0113】

ステップ813では、モバイル・デバイスが、メッシュ・ネットワークのメンバとしてそれ自体を構成することができる。たとえば、構成プロセスの一部として、モバイル・デバイスは、後の使用のためにルーティング情報を記憶することができ、メッシュ・ネットワーク内の1つまたは複数の次のホップにルーティング情報を送信することができ、メッシュ・ネットワークのピアツーピア接続を確立するためにデータを交換することができ、かつ／または暗号化鍵／暗号化解除鍵および／もしくはピアツーピア接続を介する通信に関する他の証明書を判定するために次のホップとデータを交換する（たとえば、SSLを

使用するための証明書をピアツーピア接続と交換する）ことができる。いくつかの配置では、暗号化鍵／暗号化解除鍵および／またはピアツーピア接続を介する通信に関する他の証明書は、企業管理フレームワークによって実施されるポリシー内に含められ得る。いくつかの配置では、ピアツーピア接続の確立は、ピアツーピア接続のタイプに依存する場合がある（たとえば、図7のピアツーピア接続がBLUE TOOTH（登録商標）接続である場合に、モバイル・デバイス702-Aおよびモバイル・デバイス702-Bは、接続を確立するためにペアリング・プロセスを完了することができる）。

【0114】

一特定の例では、メッシュ・ネットワークが図7の3つのモバイル・デバイスを含み、メッシュ・ネットワークが図7に示されたピアツーピア接続を使用する場合に、図7の3つのモバイル・デバイスは、次のようにメッシュ・ネットワークを使用してデータをルーティングし、送信することができる。モバイル・デバイス702-Bがそれ自体を構成した後に、モバイル・デバイス702-Bは、メッシュ・ネットワークのピアツーピア接続705を介してモバイル・デバイス702-Cにデータをルーティングし、送信することができ、メッシュ・ネットワークのピアツーピア接続703を介してモバイル・デバイス702-Aにデータをルーティングし、送信することができ、モバイル・デバイス702-Aがそれ自体を構成した後に、モバイル・デバイス702-Aは、メッシュ・ネットワークのピアツーピア接続703を介してモバイル・デバイス702-Bにデータをルーティングし、送信することができ、モバイル・デバイス702-Cがそれ自体を構成した後に、モバイル・デバイス702-Cは、メッシュ・ネットワークのピアツーピア接続705を介してモバイル・デバイス702-Bにデータをルーティングし、送信することができる。

【0115】

上で議論したように、図7は、単一のデバイスすなわちモバイル・デバイス702-Cがアクセス・ゲートウェイとの仮想プライベート・ネットワーク接続を確立した配置を示す。いくつかの変形形態では、企業モビリティ管理システムは、複数の仮想プライベート・ネットワーク接続の確立をサポートすることができる。したがって、2つ以上のデバイスが、アクセス・ゲートウェイとの仮想プライベート・ネットワーク接続を確立済みである場合がある。図9は、少なくとも2つのデバイスがアクセス・ゲートウェイとの仮想プライベート・ネットワーク接続を確立済みである、1つのそのような配置を示す。

【0116】

具体的には、図9の例の配置は、4つのモバイル・デバイス902-A、902-B、902-C、および902-Dを含む。第4のモバイル・デバイス、第2の仮想プライベート・ネットワーク接続、および第4のモバイル・デバイスの追加のピアツーピア接続の他に、図9の例の配置は、図7に関連して議論したものに類似する構成要素を含む。実際に、4つのモバイル・デバイス902-A、902-B、902-C、および902-Dは、第1の位置901（たとえば、単一の家または構内、自動車、お互いからしきい距離内、特定のサイズの地理的区域、同一のセルラ塔によってサービスされる位置など）に配置されて図示されている。各デバイスは、図5に関連して説明した企業モビリティ技術アーキテクチャの諸態様を用いて構成され得（たとえば、モバイル・デバイス502と同様に構成される）、かつ／または図6に関連して説明した企業モビリティ管理システムの諸態様を用いて構成され得る（たとえば、モバイル・デバイス602と同様に構成される）。4つのモバイル・デバイス902-A、902-B、902-C、および902-Dのそれぞれは、同一のユーザ（図示せず）に関連付けられ得る。図7に示されたモバイル・デバイスの個数は、例示のためのものである。ユーザは、より多数またはより少数のモバイル・デバイスに関連付けられ得、本明細書で説明される方法は、異なる個数のモバイル・デバイスを有する配置にあてはまる。

【0117】

ユーザは、様々な企業リソース919および／または企業サービス917にアクセスし、使用するのに4つのモバイル・デバイス902-A、902-B、902-C、および

10

20

30

40

50

902-Dのそれぞれを使用するつもりである場合がある。企業リソース919および企業サービス917へのアクセスおよびその使用は、アクセス・ゲートウェイ907によって管理され得る。アクセス・ゲートウェイ907、企業リソース919、および／または企業サービス917は、第1の位置901とは異なるまたはこれからリモートである第2の位置911に配置されたものとして図示されている。第2の位置911は、単純さのために図示されている。いくつかの配置では、企業リソース919、企業サービス919、およびアクセス・ゲートウェイ907は、お互いとは異なる位置に配置され得る。アクセス・ゲートウェイ907は、図5に関連して説明した企業モビリティ技術アーキテクチャの諸態様を用いて構成され得（たとえば、アクセス・ゲートウェイ560と同様に構成される）、かつ／または図6に関連して説明した企業モビリティ管理システムの諸態様を用いて構成され得る（たとえば、ゲートウェイ・サーバ606と同様に構成される）。企業リソース919および企業リソースは、図5および図6に関連して議論したものに類似するものとすることができる（たとえば、企業リソース504、企業サービス508、企業リソース／サービス608、609、620、622、および類似物）。アクセス・ゲートウェイ907は、企業リソース919および企業サービス917に加えて、たとえば公衆インターネット548、アプリケーション・ストア578、および類似物へのアクセスを含む機能性を提供することもできる。

【0118】

4つのモバイル・デバイス902-A、902-B、902-C、および902-Dのそれぞれは、お互いとは異なる能力を有することができ、第1の位置901で使用可能なネットワークに基づいて、あるデバイスが、アクセス・ゲートウェイ907への仮想プライベート・ネットワーク接続を確立できない場合がある。図9に示されているように、モバイル・デバイス902-Cは、アクセス・ゲートウェイ907との仮想プライベート・ネットワーク接続915を確立済みであり、モバイル・デバイス902-Dは、アクセス・ゲートウェイ907との仮想プライベート・ネットワーク接続913を確立済みである。やはり図9に示されているように、モバイル・デバイス902-Aおよび902-Bは、アクセス・ゲートウェイ907との仮想プライベート・ネットワーク接続を有しない。たとえば、モバイル・デバイス902-Cおよび902-Dは、それぞれ、これらのデバイスのそれぞれがアクセス・ゲートウェイ909と通信することを可能にする無線ネットワーク（たとえば、3G無線ネットワーク、4G無線ネットワーク、WIFI無線ローカル・エリア・ネットワーク、および類似物）に接続できるデバイスとすることができる。図9に示されているように、モバイル・デバイス902-Cおよび902-Dは、異なる無線ネットワークに接続され、モバイル・デバイス902-Cは無線ネットワーク909に接続され、モバイル・デバイス902-Dは、無線ネットワーク910に接続される（たとえば、無線ネットワーク909は、セルラ無線ネットワークとすることができ、無線ネットワーク910は、無線ローカル・アクセス・ネットワークとすることができ）。いくつかの配置では、モバイル・デバイス902-Cおよび902-Dは、同一の無線ネットワークに接続され得る。モバイル・デバイス902-Aおよび902-Bは、それぞれ、無線ネットワーク909および910に接続できないデバイス（たとえば、3G、4G、またはLTE無線ネットワークに接続する能力のないタブレット・コンピュータ）とすることができ、あるいは、ユーザが無線ネットワーク909および910に接続しないことを選択したデバイス（たとえば、機内モードにセットされたデバイスなど、使用不能にされた無線通信機を有するデバイス）とすることができる。

【0119】

仮想プライベート・ネットワーク接続913および915のそれぞれは、図5および図6に関連して議論したものと同様の、1つまたは複数のmicroVPN接続またはアプリケーション固有VPN接続とすることができる。そのような配置では、仮想プライベート・ネットワーク接続913は、アクセス・ゲートウェイ907と、たとえばモバイル・デバイス902-Dの1つまたは複数のマネージド・アプリケーション（たとえば、マネージド・アプリケーション514）および／またはモバイル・デバイス902-Dのクラ

10

20

30

40

50

イアント・エージェント（たとえば、クライアント・エージェント604）を含む、モバイル・デバイス902-Dのモビリティ管理システムの様々な構成要素との間でのデータ・トラフィックの交換を可能にすることができる。同様に、仮想プライベート・ネットワーク接続915は、アクセス・ゲートウェイ907と、たとえばモバイル・デバイス902-Cの1つまたは複数のマネージド・アプリケーション（たとえば、マネージド・アプリケーション514）および／またはモバイル・デバイス902-Cのクライアント・エージェント（たとえば、クライアント・エージェント604）を含む、モバイル・デバイス902-Cのモビリティ管理システムの様々な構成要素との間でのデータ・トラフィックの交換を可能にすることができる。仮想プライベート・ネットワーク接続913は、無線ネットワーク910（および、図9に明示的には図示されていない1つまたは複数の他のネットワーク）を通るトンネルとして働くことができる。同様に、仮想プライベート・ネットワーク接続915は、無線ネットワーク909（および、図9に明示的には図示されていない1つまたは複数の他のネットワーク）を通るトンネルとして働くことができる。仮想プライベート・ネットワーク接続913および914を介するデータの交換に適するマネージド・アプリケーションおよび／またはクライアント・エージェントのタイプのいくつかの例は、たとえば、Citrix System, Inc. によるアプリケーションのWORX suite（たとえば、Citrix Systems, Inc. によるWORX HOME、Citrix Systems, Inc. によるWORXMAILなど）、およびCitrix Systems, Inc. によるXENMOBILEと互換の他のアプリケーション／クライアント・エージェントを含む。

【0120】

4つのモバイル・デバイス902-A、902-B、902-C、および902-Dは、メッシュ・ネットワークのメンバ（またはノード）として構成され得る。図7に関連して議論された配置と同様に、明瞭さおよび議論のしやすさのために、本開示は、ルーティング技法を使用するメッシュ・ネットワークの例を提供する。したがって、図9に示されているように、モバイル・デバイス902-A、902-B、902-C、および902-Dは、メッシュ・ネットワークのメンバであり、データは、ピアツーピア接続903、904、905、および906を介してメッシュ・ネットワーク全体にルーティングされ得る。ピアツーピア接続903、904、905、および906は、たとえばBLUETOOTH（登録商標）プロトコル、WIFI DIRECTプロトコル、または物理的に非常に近接したデバイスの間の直接通信を可能にする任意の他のプロトコルを含む、1つまたは複数のトランスポート・プロトコルを使用することができる（たとえば、ピアツーピア接続905および906が、BLUETOOTH（登録商標）プロトコルを使用することができ、ピアツーピア接続903および904が、WIFI DIRECTプロトコルを使用することができる）。ピアツーピア接続903、904、905、および906を介して送信されるデータは、1つまたは複数の暗号化方式に基づいて暗号化され得る。さらに、モバイル・デバイス902-A、902-B、902-C、および902-Dの間に追加のピアツーピア接続がある場合がある。たとえば、ピアツーピア接続（図示せず）が、モバイル・デバイス902-Aとモバイル・デバイス902-Dとの間に確立され得る。別の例として、図示されたピアツーピア接続904に加えて、第2のピアツーピア接続（図示せず）が、モバイル・デバイス902-Aとモバイル・デバイス902-Cとの間に確立され得る。メッシュ・ネットワークの使用は、例示のためのものである。他のタイプのアドホック・ネットワークまたはピアツーピア・ネットワークが、本明細書で説明される諸態様を組み込んだ様々な実施形態内で使用され得る。メッシュ・ネットワークのメンバになるために各モバイル・デバイス902-A、902-B、902-Cおよび902-Dによって使用され得る例の方法が、下で図10Aに関連して議論される。2つの仮想プライベート・ネットワーク接続913および914のどちらが使用されるのかを管理するのに使用され得る例の方法が、下で図10Bに関連して議論される。メッシュ・ネットワークの確立に関するさらなる詳細は、図12に関連して議論される。

【0121】

図示の配置は、モバイル・デバイス 902-A および 902-B からのデータがアクセス・ゲートウェイ 907 によって受信されることを可能にすることができる。この形で、モバイル・デバイス 902-A および 902-B は、企業リソース 919 および企業サービス 917 を含むアクセス・ゲートウェイ 907 によって制御され、かつ／または管理される機能性にアクセスし、かつ／または使用することができる可能性がある。たとえば、アクセス・ゲートウェイ 907 用のデータ（たとえば、モバイル・デバイス 902-A および 902-B のマネージド・アプリケーションまたはクライアント・エージェントによって生成されたデータ）は、メッシュ・ネットワークの 1 つまたは複数のピアツーピア接続 903～906 を介して、アクセス・ゲートウェイ 907 との接続を確立済みのモバイル・デバイス（たとえば、モバイル・デバイス 902-C またはモバイル・デバイス 902-D）にルーティングされ、送信され得る。確立された仮想プライベート・ネットワーク接続を有するモバイル・デバイスによって受信された後に、データは、その仮想プライベート・ネットワーク接続を介してアクセス・ゲートウェイ 907 に送信され得る（たとえば、データがモバイル・デバイス 902-D にルーティングされた場合には仮想プライベート・ネットワーク接続 913 を介し、データがモバイル・デバイス 902-C にルーティングされた場合には仮想プライベート・ネットワーク接続 915 を介して）。アクセス・ゲートウェイ 907 は、モバイル・デバイス 902-A または 902-B 用のデータ（たとえば、企業リソース 919 または企業サービス 917 のアクセスに基づいて生成されたデータ）を、仮想プライベート・ネットワーク接続を介して、確立された仮想プライベート・ネットワーク接続を有するモバイル・デバイスに送信することができる。確立された仮想プライベート・ネットワーク接続を有するモバイル・デバイスによって受信された後に、データは、メッシュ・ネットワークの 1 つまたは複数のピアツーピア接続 903～906 を介して所期の宛先にルーティングされ、送信され得る。受信時に、モバイル・デバイス 902-A または 902-B は、アプリケーション管理フレームワークに従ってデータを処理することができる（たとえば、マネージド・アプリケーションにデータを供給する、データをコンテナ内に記憶するなど）。たとえば、モバイル・デバイス 902-B のマネージド・メール・アプリケーションは、ユーザが仮想プライベート・ネットワーク接続 913 を使用して新しい電子メールを受信することを可能にするために、アクセス・ゲートウェイ 907 を介して電子メール・データを受信することができる。別の例として、モバイル・デバイス 902-A のマネージド・ブラウザ・アプリケーションは、ユーザが仮想プライベート・ネットワーク接続 913 を使用してモバイル・デバイス 902-A からインターネットをブラウズすることを可能にするために、アクセス・ゲートウェイからウェブ・ブラウジング・データを受信できる可能性がある。さらに、メッシュ・ネットワークは、モバイル・デバイス 902-A、902-B、902-C、および 902-D がアプリケーション管理フレームワークに関する様々な機能を実行することを可能にするのできるデータをこれらのモバイル・デバイスの間で送信するのに使用され得る。たとえば、ユーザがモバイル・デバイス 902-A、902-B、902-C、および 902-D のうちの 1 つからのスクリーンを共有することを可能にするために、スクリーン共有データがこれらのデバイスの間で送信され得る。別の例として、ユーザがモバイル・デバイス 902-A、902-B、902-C、および 902-D の間で電子メール・メッセージを同期化することを可能にするために、電子メール・データが、モバイル・デバイス 902-A、902-B、902-C、および 902-D の間で送信され得る。メッシュ・ネットワークが企業モビリティ管理システムに関連してどのように使用され得るのかに関するさらなる詳細は、図 11A～図 11D および図 12 に関連して議論される。

【0122】

図 10A は、メッシュ・ネットワークの確立に関連して使用され得る別の例の方法を示す。具体的には、図 10A の例の方法は、メッシュ・ネットワークのメンバになるか他の形でメッシュ・ネットワークを確立するのに図 9 のモバイル・デバイス 902-A、902-B、902-C、および 902-D のそれぞれによって使用され得る。いくつかの配置では、図 10A のステップは、たとえば図 6 のクライアント・エージェント 604 を含

む企業モビリティ管理システムの1つまたは複数の構成要素によって実行され得る。さらに、モバイル・デバイスは、メッシュ・ネットワークの確立を容易にするために、モバイル・デバイスの存在および近くのデバイスの発見をアダプタイズするのを援助するためにOPENGARDEN SDKなどの既存技術の変形形態を使用することができる。

【0123】

ステップ1001では、モバイル・デバイスが、1つまたは複数の他のモバイル・デバイスの1つまたは複数のアダプタイズメントを受信することができる。ステップ1001は、図8のステップ805と同様に実行され得る。たとえば、1つまたは複数の他のモバイル・デバイスのアダプタイズメントは、他のモバイル・デバイスの存在をモバイル・デバイスに示すことができ、トランスポート・プロトコルに固有とすることができる。1つまたは複数のアダプタイズメントは、1つまたは複数のピアツーピア通信を介して受信され得る（たとえば、アダプタイズメントは、ステップ1001でBLUETOOTH（登録商標）通信および／またはWIFI DIRECT通信を介して受信され得る）。いくつかの配置で、ステップ1001で受信される1つまたは複数のアダプタイズメントは、1つまたは複数の他のモバイル・デバイスのユーザ情報を含むことができる（たとえば、モバイル・デバイス902-Bのアダプタイズメントは、モバイル・デバイス902-Bのユーザによって選択されたセキュリティ証明書を含むことができる）。さらに、ステップ1001で受信される1つまたは複数のアダプタイズメントは、アクセス・ゲートウェイへの仮想プライベート・ネットワーク接続がアダプタイズメントの特定のソース・デバイスのために確立済みであるかどうかに関する指示を含むことができる（たとえば、モバイル・デバイス902-Bのアダプタイズメントは、仮想プライベート・ネットワーク接続が確立されていないことを示すことができ、モバイル・デバイス902-Cのアダプタイズメントは、仮想プライベート・ネットワーク接続が確立されていることを示すことができる）。

【0124】

図示の配置では、この方法は、ステップ1001での1つまたは複数のアダプタイズメントの受信に応答してステップ1003に進むことができる。いくつかの配置（図10Aには図示せず）では、モバイル・デバイスは、直接にステップ1003に進む前に、メッシュ・ネットワークのメンバになるための認証が以前に受信されたかどうかを判定することができる。この判定は、たとえば、モバイル・デバイスのクライアント・エージェントのメッシュ・ネットワーク・セッティングの値（たとえば、メッシュ・ネットワーク・セッティングが、メッシュ・ネットワークのメンバシップがユーザによって認可されることを示すかどうか）に基づいて、または、モバイル・デバイスがSSOのために構成された有効な認証トークンを記憶することに基づいて、実行され得る。認可が以前に受信されなかった場合には、モバイル・デバイスは、認可についてユーザにプロンプトを出すことができる。認可が以前に受信された場合には、この方法は、ステップ1003に進むことができる。

【0125】

ステップ1003では、モバイル・デバイスが、モバイル・デバイスの1つまたは複数のアダプタイズメントを送信することができる。このステップは、ステップ1003が、モバイル・デバイスがステップ1001でアダプタイズメントを受信することに応答してまたはこれに基づいて実行されると考えられることを除いて、図8のステップ801と同様に実行され得る。いくつかの配置で、ステップ1003で送信される各アダプタイズメントは、モバイル・デバイスのユーザ情報（たとえば、モバイル・デバイス902-Dのユーザによって選択されたセキュリティ証明書）を含むことができる。さらに、ステップ1003で送信される1つまたは複数のアダプタイズメントは、アクセス・ゲートウェイへの仮想プライベート・ネットワーク接続がモバイル・デバイスのために確立済みであるかどうかに関する指示を含むことができる。

【0126】

ステップ1005では、モバイル・デバイスが、ステップ1001で受信された1つま

たは複数のアドバタイズメントに基づいて1つまたは複数の他のモバイル・デバイスのユーザ情報を判定することができる。このステップは、図8のステップ807と同様に実行され得る（たとえば、ステップ1001で受信されたアドバタイズメントからユーザ情報を抽出する、1つまたは複数のユーザ・デバイスにユーザ情報要求を送信するなど）。さらに、いくつかの配置では、ユーザ情報の判定に加えてまたはその代替案として、モバイル・デバイスは、仮想プライベート・ネットワーク接続が1つまたは複数の他のデバイスのために確立済みであるかどうかに関する指示を判定することができる（たとえば、ステップ1001で受信されたアドバタイズメントから指示を抽出する、1つまたは複数の他のデバイスに指示の要求を送信する、1つまたは複数の他のデバイスに指示およびユーザ情報の1つまたは複数の要求を送信する（要求のそれぞれは、指示およびユーザ情報の要求である）など）。

10

【0127】

ステップ1007では、モバイル・デバイスが、メッシュ・ネットワークのメンバシップを認証すべきかどうかを判定することができる。このステップは、図8のステップ809と同様に実行され得る（たとえば、1つまたは複数の他のデバイスのユーザ情報およびモバイル・デバイスのユーザ情報に基づいて判定を実行する、モバイル・デバイスおよび一致するユーザ情報を有する1つまたは複数のモバイル・デバイスに基づいて判定を実行するなど）。メッシュ・ネットワークのメンバシップを認証すべきであるとの判定時に、この方法は、ステップ1009に進むことができる。モバイル・デバイスが、メッシュ・ネットワークのメンバシップを認証すべきではないと判定する（たとえば、他のモバイル・デバイスのユーザ情報のいずれもが、モバイル・デバイスのユーザ情報と一致しない）場合には、この方法は終了する。

20

【0128】

ステップ1009では、モバイル・デバイスが、複数（たとえば、2つ以上）の仮想プライベート・ネットワーク接続が、メッシュ・ネットワークのメンバになるデバイスの間で確立済みであるかどうかを判定することができる。たとえば、例示のために図9に示された配置を使用すると、モバイル・デバイス902-A~902-Dは、すべてがメッシュ・ネットワークのメンバシップに関して認証され得、モバイル・デバイス902-Dは、モバイル・デバイス902-A、902-B、および902-Cのそれぞれから、仮想プライベート・ネットワーク接続がそれぞれのデバイスのために確立済みであるかどうかに関する指示を受信済みである場合があり、モバイル・デバイス902-Dは、仮想プライベート・ネットワークがモバイル・デバイス902-Dのために確立済みであるかどうかに関する指示へのアクセスを有することができる。メッシュ・ネットワークのメンバの指示のうちの少なくとも2つ（たとえば、モバイル・デバイス902-A、902-B、および902-Cの指示とモバイル・デバイス902-Dの指示と）が、仮想プライベート・ネットワーク接続が確立済みであることを示す指示を提供する場合には、モバイル・デバイス902-Dは、複数の仮想プライベート・ネットワーク接続が確立済みであると判定することができる。1つまたはより少数のメッシュ・ネットワークのメンバの指示が、仮想プライベート・ネットワーク接続が確立済みであることを示す指示を提供する場合には、モバイル・デバイス902-Dは、複数の仮想プライベート・ネットワーク接続が確立済みではないと判定することができる。図9に示された特定の配置に注意を向けると、モバイル・デバイスは、モバイル・デバイス902-Cと902-Dとの両方が、仮想プライベート接続が確立済みであることを示す指示を提供するので、複数の仮想プライベート・ネットワーク接続が確立済みであると判定することができる。

30

40

【0129】

複数の仮想プライベート・ネットワーク接続が確立済みであるとの判定時に、この方法は、ステップ1011に進むことができる。モバイルが、複数の仮想プライベート・ネットワーク接続が確立済みではないと判定する場合には、この方法はステップ1015に進むことができる。

【0130】

50

ステップ1011では、複数の仮想プライベート・ネットワーク接続のどれが、メッシュ・ネットワークを介して受信された、アクセス・ゲートウェイ用のデータに使用されるのかを、モバイル・デバイスが選択することができる。モバイル・デバイスは、複数の仮想プライベート・ネットワーク接続に関する測定値の比較に基づいてこの選択を実行することができる。いくつかの配置で、選択は、複数の仮想プライベート・ネットワーク接続のどれが最高速と判定されるのかに基づくものとして行うことができる。たとえば、確立された仮想プライベート・ネットワーク接続を有する各モバイル・デバイスは、確立された仮想プライベート・ネットワーク接続の1つまたは複数の測定値（たとえば、仮想プライベート・ネットワークの平均のまたは瞬間的な帯域幅測定値、アクセス・ゲートウェイとの接続上での瞬間的なまたは平均のping時間など）を提供することができる。これらの測定値に基づいて、モバイル・デバイスは、複数の仮想プライベート・ネットワーク接続のうちの1つを選択することができる（たとえば、最大の帯域幅を有する仮想プライベート・ネットワークを選択する、最短のping時間を有する仮想プライベート・ネットワークを選択する、帯域幅とping時間との重み付きの組み合わせに基づくなど）。1つまたは複数の測定値は、仮想プライベート・ネットワーク接続が確立済みであることまたはモバイル・デバイスによる別々の要求に応答したことを示す指示と一緒に供給され得る。図9に示された配置を使用する特定の例として、モバイル・デバイス902-Cは、モバイル・デバイス902-Dへの仮想プライベート・ネットワーク接続915を介するアクセス・ゲートウェイ907のアクセスに関して5ミリ秒のping時間を提供した可能性があり、モバイル・デバイス902-Dは、仮想プライベート・ネットワーク接続913を介するアクセス・ゲートウェイ907のアクセスに関して10ミリ秒のping時間を測定した可能性がある。したがって、モバイル・デバイス902-Dは、より短いping時間に基づいて、メッシュ・ネットワークを介して受信された、アクセス・ゲートウェイ用のデータに使用される接続として仮想プライベート・ネットワーク接続915を選択することができる。

【0131】

ステップ1013では、モバイル・デバイスが、選択された仮想プライベート・ネットワーク接続の状況を監視するプロセスを開始できる。選択された仮想プライベート・ネットワーク接続の状況を監視するプロセスに関するさらなる詳細は、図10Bに関して議論される。

【0132】

ステップ1015では、モバイル・デバイスが、1つまたは複数の他のモバイル・デバイスのうちの少なくとも1つにデータをルーティングするのに使用可能であるルーティング情報を判定することができる。このステップは、図8のステップ811と同様に実行され得る。さらに、ルーティング情報は、どの仮想プライベート・ネットワーク接続がステップ1011で選択されたのかに基づいて判定され得る。たとえば、図10に示された例示的な配置を使用し、仮想プライベート・ネットワーク接続913がステップ1011で選択されたと仮定すると、モバイル・デバイス902-Aからモバイル・デバイス902-Cによって受信されたデータが、アクセス・ゲートウェイ907用である場合に、そのデータがモバイル・デバイス902-Dにルーティングされなければならないことを示すために、ルーティング情報が判定され得る。

【0133】

ステップ1017では、モバイル・デバイスが、メッシュ・ネットワークのメンバとしてそれ自体を構成することができる。このステップは、図8のステップ813と同様に実行され得る。たとえば、構成プロセスの一部として、モバイル・デバイスは、後の使用のためにルーティング情報を記憶することができ、メッシュ・ネットワーク内の1つまたは複数の次のホップにルーティング情報を送信することができ、メッシュ・ネットワークのピアツーピア接続を確立するためにデータを交換することができ、かつ／またはピアツーピア接続を介する通信に関する暗号化鍵を判定するために次のホップとデータを交換することができる。さらに、ルーティング情報が、どの仮想プライベート・ネットワーク接続

がステップ1011で選択されたのかに基づくことに鑑みて、モバイル・デバイスによって実行される構成は、どの仮想プライベート・ネットワーク接続がステップ1011で選択されたのかに基づいて実行され得る。

【0134】

一特定の例では、メッシュ・ネットワークが図9の4つのモバイル・デバイスを含み、メッシュ・ネットワークが図9に示されたピアツーピア接続を使用する場合に、図9の4つのモバイル・デバイスは、次のようにメッシュ・ネットワークを使用してデータをルーティングし、送信することができる。モバイル・デバイス902-Aがそれ自体を構成した後に、モバイル・デバイス902-Aは、メッシュ・ネットワークのピアツーピア接続903を介してモバイル・デバイス902-Bにデータをルーティングし、送信することができ、メッシュ・ネットワークのピアツーピア接続904を介してモバイル・デバイス902-Cにデータをルーティングし、送信することができ、モバイル・デバイス902-Bがそれ自体を構成した後に、モバイル・デバイス902-Bは、メッシュ・ネットワークのピアツーピア接続903を介してモバイル・デバイス702-Aにデータをルーティングし、送信することができ、メッシュ・ネットワークのピアツーピア接続906を介してモバイル・デバイス902-Dにデータをルーティングし、送信することができ、モバイル・デバイス902-Cがそれ自体を構成した後に、モバイル・デバイス902-Cは、メッシュ・ネットワークのピアツーピア接続904を介してモバイル・デバイス902-Aにデータをルーティングし、送信することができ、メッシュ・ネットワークのピアツーピア接続905を介してモバイル・デバイス902-Dにデータをルーティングし、送信することができ、モバイル・デバイス902-Dがそれ自体を構成した後に、モバイル・デバイス902-Dは、メッシュ・ネットワークのピアツーピア接続905を介してモバイル・デバイス902-Cにデータをルーティングし、送信することができ、メッシュ・ネットワークのピアツーピア接続906を介してモバイル・デバイス902-Bにデータをルーティングし、送信することができる。

【0135】

上の議論に鑑みて、一般に、図10Aの例の方法は、図8に関連して議論したものに類似する複数のステップを含む。しかし、図10Aの例の方法は、図8に関連して議論したステップの代替物またはこれに対する追加と考えることのできる様々なステップおよび／またはステップの配置を含む。たとえば、図10Aのステップ1001および1003は、いくつかの実施形態で、ステップ801、803、および805の代わりに使用され得る。別の例として、ステップ1009、1011、1013、および1015は、いくつかの実施形態で、図8の例の方法に追加され得る。さらなる別の例として、図8のステップ801は、図10Aの例の方法で実行されるステップに加えて実行され得る。

【0136】

さらに、モバイル・デバイスは、図8および図10Aに関連して説明した方法の1つまたは複数の異なる変形形態を実行するように構成され得る。たとえば、各モバイル・デバイスは、モバイル・デバイスがピアツーピア通信を介してアドバタイズメントを受信する前にユーザがメッシュ・ネットワークを確立する試みを開始するかどうかに基づいて、メッシュ・ネットワークの確立に関連して使用され得る2つの方法の一方を実行するように構成され得る。実際に、図9の例示的な配置を使用する特定の例として、ユーザは、モバイル・デバイス902-D上のユーザ・インターフェースと対話し、モバイル・デバイスがメッシュ・ネットワークの確立を試みることを開始しまたは他の形でこれを引き起こすボタンを押す（メニュー・オプションを選択し、または他の形でセッティングを変更する）ことができる。したがって、モバイル・デバイス902-Dは、ユーザの開始に基づいて図8のステップ801～805を実行し、その後、ステップ1005で開始する図10Aの方法の実行に進むことができる。モバイル・デバイス902-Dで実行される方法に基づいて、他のモバイル・デバイス（たとえば、モバイル・デバイス902-A、902-B、および902-C）は、モバイル・デバイス902-Dからアドバタイズメントを受信することができる。モバイル・デバイス902-A、902-B、および902-C

のそれぞれは、ユーザがデバイス 902-A、902-B、および 902-C 上でメッシュ・ネットワークを確立する試みを開始する前にデバイス 902-A、902-B、および 902-C がアダプタイズメントを受信することに基づいて、10A の方法の実行に進むことができる。図 8 および図 10A の上で説明した変形形態は、実施形態がメッシュ・ネットワークの確立に関連して使用できる多数の変形形態の少数の例にすぎない。

【0137】

図 10B は、メッシュ・ネットワークの管理に関連して使用され得る例の方法を示す。詳細には、図 10B は、選択された仮想プライベート・ネットワーク接続の状況を監視するための例の方法を示す。具体的には、図 10B の例の方法は、選択された仮想プライベート・ネットワーク接続の状況を監視するために図 9 からのモバイル・デバイス 902-A、902-B、902-C、および 902-D のそれぞれによって使用され得る。いくつかの配置では、図 10B のステップは、たとえば図 6 のクライアント・エージェント 604 を含む、企業モビリティ管理システムの 1 つまたは複数の構成要素によって実行され得る。

【0138】

ステップ 1021 では、モバイル・デバイスは、仮想プライベート・ネットワーク接続の 1 つまたは複数の測定値を示すデータを受信することができる。このデータは、仮想プライベート・ネットワーク接続の性能を示すことができる（たとえば、仮想プライベート・ネットワークの平均のまたは瞬間的な帯域幅測定値、アクセス・ゲートウェイとの接続上での瞬間的なまたは平均の ping 時間など）。その代わりにまたはそれに加えて、このデータは、仮想プライベート・ネットワーク接続が障害を発生したことを示すことができる。ステップ 1021 で受信されるデータは、モバイル・デバイスによって送信された、1 つまたは複数の測定値の要求に応答して受信され得る。このデータは、周期的スケジュールに基づいても受信され得る（たとえば、確立された仮想プライベート・ネットワーク接続を有するモバイル・デバイスは、1 つまたは複数の測定値を判定し、5 秒おき、5 分おき、毎時、その他など、周期的にそのデータを送信することができる）。このデータは、さらに、仮想プライベート・ネットワーク接続の性能が所定のしきい値を超えて変化したとデバイスが判定することに基づいて受信され得る（たとえば、確立された仮想プライベート・ネットワーク接続を有するモバイル・デバイスは、確立された接続が障害を発生したと判定した後にデータを送信することができ、帯域幅測定値が指定された量のメガビット毎秒だけ減少したと判定した時にデータを送信することができ、ping 時間が指定されたミリ秒数だけ増加したと判定した時にデータを送信することができるなど）。特定の例として、図 9 の例示的な配置を使用すると、モバイル・デバイス 902-D は、仮想プライベート・ネットワーク接続 915 の 1 つまたは複数の測定値を示すデータを、ステップ 1021 でピアツーピア接続 905 を介してモバイル・デバイス 902-C から受信することができる。

【0139】

ステップ 1023 では、モバイル・デバイスが、選択された仮想プライベート・ネットワーク接続を変更すべきかどうかを判定することができる。たとえば、この判定は、選択された仮想プライベート・ネットワーク接続と他の確立された仮想プライベート・ネットワーク接続との測定値の比較に基づくものとして行うことができる。この比較は、図 10A のステップ 1011 に関連して議論した比較と同様に実行され得る。特定の例として、図 9 の例示的な配置を使用し、仮想プライベート・ネットワーク接続 915 が、現在選択されている仮想プライベート・ネットワーク接続であると仮定すると、モバイル・デバイス 902-C は、モバイル・デバイス 902-D への仮想プライベート・ネットワーク接続 915 を介するアクセス・ゲートウェイ 907 のアクセスに関して 30 ミリ秒の ping 時間を最も最近に提供した可能性があり、モバイル・デバイス 902-D は、仮想プライベート・ネットワーク接続 913 を介するアクセス・ゲートウェイ 907 のアクセスに関して 10 ミリ秒の ping 時間を最も最近に測定した可能性がある。したがって、モバイル・デバイス 902-D は、仮想プライベート・ネットワーク接続 913 のより短い pin

g 時間に基づいて、選択された仮想プライベート・ネットワーク接続が、仮想プライベート・ネットワーク接続 913 に変更されなければならないと判定することができる。

【0140】

選択された仮想プライベート・ネットワーク接続が変化しなければならないと判定する時に、この方法はステップ 1025 に進むことができる。モバイル・デバイスが、選択された仮想プライベート・ネットワーク接続が変化してはならないと判定する時に、この方法は終了することができる。

【0141】

ステップ 1025 では、モバイル・デバイスが、選択された仮想プライベート・ネットワーク接続が変化したことを示す 1 つまたは複数のメッセージを送信することができる。10
いくつかの配置では、1 つまたは複数のメッセージは、メッシュ・ネットワークの各メンバが変化について通知されるようにするために送信される。メッセージの受信時に、メッシュ・ネットワークの各メンバは、選択された仮想プライベート・ネットワーク接続の変化に基づいて、その構成の更新に進むことができる。たとえば、図 9 の例示的な配置を使用し、仮想プライベート・ネットワーク接続 913 が、新たに選択された仮想プライベート・ネットワーク接続であると仮定すると、モバイル・デバイス 902-A、902-B、および 902-C は、選択された VPN 接続が変化したことを示すメッセージをそれぞれ送信され得、モバイル・デバイス 902-A、902-B、および 902-C のそれぞれは、アクセス・ゲートウェイ 907 用のデータがモバイル・デバイス 902-C にルーティングされるようにするために、メッセージの受信にตอบสนองして、選択された仮想プライベート・ネットワーク接続の変化に基づいて、その構成を更新することができる（たとえば、記憶されたルーティング情報および類似物を更新する）。20

【0142】

ステップ 1027 では、モバイル・デバイスが、選択された仮想プライベート・ネットワーク接続の変化に基づいて、その構成を更新することができる。たとえば、モバイル・デバイスは、アクセス・ゲートウェイ用のデータが新たに選択された仮想プライベート・ネットワーク接続を介してアクセス・ゲートウェイに送信され得るようにするためにそのデータがルーティングされるようにするために、記憶されたルーティング情報および他の構成セッティングを更新することができる。ステップ 1025 で議論した特定の例を継続すると、モバイル・デバイス 902-D は、アクセス・ゲートウェイ 907 用のデータがピアツーピア接続 905 を使用してモバイル・デバイス 902-C にルーティングされるようにするために、その構成を更新することができる。30

【0143】

図 11A～図 11D は、本明細書で説明される様々な態様に従ってメッシュ・ネットワークの使用に関連して使用され得る例の方法を示す。具体的には、図 11A～図 11D の例の方法は、図 7 および図 9 に示されたモバイル・デバイスによって、メッシュ・ネットワークを確立した後に企業モビリティ管理システムに関連する様々な機能を実行するのに使用され得る。いくつかの配置では、図 11A～図 11D の例の方法全体で示される様々なステップは、たとえば図 6 のクライアント・エージェント 604 ならびに／または図 5 および図 6 のマネージド・アプリケーションを含む、企業モビリティ管理システムの 1 つまたは複数の構成要素によって実行され得る。さらに、モバイル・デバイスは、メッシュ・ネットワークのメンバの間でのデータのルーティングを援助するために OPENGARDEN SDK などの既存技術の変形形態を使用することができる。図 11A～図 11D の例の方法に基づいて実行され得る様々な機能に関するさらなる詳細は、図 12 で議論される。40

【0144】

図 11A は、モバイル・デバイスが、それが生成するデータをメッシュ・ネットワークを介して送信できる例の方法を示す。

【0145】

ステップ 1101 では、モバイル・デバイスが、データがメッシュ・ネットワークを介

50

して送信されるべきであると判定することができる。この判定は、たとえばクライアント・デバイス上のマネージド・アプリケーションまたはクライアント・エージェントによって実行され得る。さらに、この判定は、マネージド・アプリケーションを実行する時または企業モビリティ管理システムの機能性を提供する時に実行される様々なタイプのデータ処理に基づいて実行され得る。たとえば、この判定は、マネージド・アプリケーションがアクセス・ゲートウェイ用のデータを生成することに基づいて、メッシュ・ネットワークの別のメンバ用のデータの生成に基づいて、および／またはセキュア・コンテナからのデータの取出に基づいて、実行され得る。より特定の例として、マネージド電子メール・アプリケーションは、メッシュ・ネットワーク上のメンバの電子メールの同期化を試みるメール同期化プロセスをたどることができる。したがって、データは、電子メール同期化の試みの指示および／またはメール同期化プロセスを完了するのに必要な電子メール・データを含むことができる。別のより特定の例として、マネージド・アプリケーションは、アクセス・ゲートウェイを介してアクセス可能な企業リソースまたは企業サービスにアクセスする要求を示すデータを生成することができる。したがって、このデータは、要求の指示、どのリソースまたはサービスが要求されているのかの指示、および／または要求を完了するのに必要である可能性がある任意のセキュリティ証明書（たとえば、SSOのために構成された有効な認証トークン、ユーザ名／パスワードなど）を含むことができる。

10

【0146】

メッシュ・ネットワークを介して送信されるべきデータを判定した後に、この方法は、モバイル・デバイスが1つまたは複数のピアツーピア接続を介してステップ1101で判定されたデータを送信することを可能にするのできる反復プロセスを示す図11Aのステップ1103～1109に進むことができる。たとえば、図9の例示的な配置を使用すると、ステップ1103～1109によって表される反復プロセスは、モバイル・デバイス902-Aが、ピアツーピア接続903および／またはピアツーピア接続904を介してメッシュ・ネットワーク内の次のホップにデータを送信することを可能にすることができる。

20

【0147】

ステップ1103では、モバイル・デバイスが、メッシュ・ネットワーク内の次のホップのために確立されるピアツーピア接続のタイプを判定することができる。この判定は、モバイル・デバイスによって記憶されるメッシュ・ネットワークのルーティング情報および／またはモバイル・デバイスによってメッシュ・ネットワークメンバとしてのその構成に関連して記憶される任意の他の情報に基づくものとすることができる。たとえば、図9の例示的な配置を使用すると、モバイル・デバイス902-Aは、モバイル・デバイス902-Bへの次のホップに関して、ピアツーピア接続がBLUETOOTH（登録商標）接続であると判定することができる。代替の例として、モバイル・デバイス902-Bは、モバイル・デバイス902-Dへの次のホップに関して、ピアツーピア接続がWIFI DIRECT接続であると判定することができる。

30

【0148】

ステップ1105では、モバイル・デバイスが、ピアツーピア接続のタイプに基づいて、メッシュ・ネットワークを介して送信されるべきデータを処理することができる。たとえば、ピアツーピア接続のタイプがBLUETOOTH（登録商標）接続であると判定される場合に、ステップ1101で判定されたデータは、BLUETOOTH（登録商標）プロトコルに従うように処理され得る。別の例として、ピアツーピア接続のタイプがWIFI DIRECT接続であると判定される場合に、ステップ1101で判定されたデータは、WIFI DIRECTプロトコルに従うように処理され得る。

40

【0149】

さらに、データの処理は、ピアツーピア接続を介してデータを通信するのに必要な暗号化方式に従ってデータを暗号化することを含むことができる。たとえば、いくつかの変形形態では、暗号化鍵は、企業管理フレームワークのポリシーから取り出され、データを暗号化するのに使用され得る。他の変形形態では、暗号化鍵は、モバイル・デバイスがメッシ

50

ユ・ネットワークのメンバとしてそれ自体を構成した時（たとえば、図8のステップ813および図10Aのステップ1017）に判定済みである場合があり、その暗号化鍵が、データを暗号化するのに使用され得る。

【0150】

ステップ1107では、モバイル・デバイスが、処理されたデータをピアツーピア接続を介して送信することができる。たとえば、モバイル・デバイスは、ステップ1105に由来する処理されたデータを、1つまたは複数のBLUETOOTH（登録商標）通信を使用して、BLUETOOTH（登録商標）接続を介して送信することができる。別の例として、モバイル・デバイスは、ステップ1105に由来する処理されたデータを、1つまたは複数のWIFI DIRECT通信を使用して、WIFI DIRECT接続を介して送信することができる。より特定の例では、図9の例示的な配置を使用すると、モバイル・デバイス902-Aは、ピアツーピア接続903を介してモバイル・デバイス902-Bに、ステップ1101で判定されたデータを含む1つまたは複数のBLUETOOTH（登録商標）通信を送信することができる。

10

【0151】

ステップ1109では、モバイル・デバイスが、データが追加のピアツーピア接続を介して送信される必要があるかどうかを判定することができる。いくつかの配置では、これは、次のホップのうちの1つへの追加のピアツーピア接続が確立済みであるかどうかを判定し、ステップ1101で判定されたデータがそのピアツーピア接続にまだ送信されていないと判定するために、ルーティング情報を解析することを含むことができる。たとえば、図9の例示的な配置を使用すると、モバイル・デバイス902-Aは、ルーティング情報に基づいてピアツーピア接続904を識別することと、ステップ1101で判定されたデータがピアツーピア接続904を介して送信済みではないと判定することとによって、この判定を実行することができる。データが追加のピアツーピア接続を介して送信される必要があると判定する時に、この方法は、ステップ1103～1109によって表される反復プロセスを繰り返すために（たとえば、ピアツーピア接続904のために繰り返される）、ステップ1103に戻って進むことができる。データが追加のピアツーピア接続を介して送信される必要がないと判定する時に、この方法は終了することができる。

20

【0152】

図11Bは、モバイル・デバイスが、それがピアツーピア接続を介して受信するデータをメッシュ・ネットワークの次のホップにルーティングできる、例の方法を示す。

30

【0153】

ステップ1121では、モバイル・デバイスが、メッシュ・ネットワークのピアツーピア接続を介してデータを受信することができる。このデータは、ピアツーピア接続のタイプに従う1つまたは複数の通信内で受信され得る。たとえば、ピアツーピア接続がBLUETOOTH（登録商標）接続である場合には、データは、1つまたは複数のBLUETOOTH（登録商標）通信内で受信され得る。ピアツーピア接続がWIFI DIRECT接続である場合には、データは、1つまたは複数のWIFI DIRECT通信内で受信され得る。一特定の例では、図9の例示的な配置を使用すると、モバイル・デバイス902-Bは、ピアツーピア接続903を介して、メッシュ・ネットワークを介して送信されるべきデータ（たとえば、図11Aのステップ1101で判定されたデータ）を含む1つまたは複数のBLUETOOTH（登録商標）通信を受信することができる。いくつかの配置で、このデータは、図11Bの次のステップに進む前に暗号化解除される必要がある場合がある。

40

【0154】

ステップ1122では、モバイル・デバイスが、ステップ1121で受信されたデータを処理することができる。たとえば、データの処理は、データをそのトランスポート・パケットから抽出することを含むことができる（たとえば、1つまたは複数のBLUETOOTH（登録商標）パケットからデータを抽出する、1つまたは複数のWIFI DIRECTパケットからデータを抽出するなど）。さらに、データの処理は、ピアツーピア

50

接続を介してデータを通信するのに必要な暗号化方式に従ってデータを暗号化解除することを含むことができる。たとえば、いくつかの変形形態で、暗号化解除鍵は、企業管理フレームワークのポリシーから取り出され、データを暗号化解除するのに使用され得る。他の変形形態では、暗号化解除鍵は、モバイル・デバイスがメッシュ・ネットワークのメンバーとしてそれ自体を構成した時（たとえば、図8のステップ813および図10Aのステップ1017）に判定済みである場合があり、その暗号化解除鍵が、データを暗号化解除するのに使用され得る。

【0155】

ステップ1123では、モバイル・デバイスが、ステップ1121で受信され、ステップ1122で処理されたデータがモバイル・デバイス用であるかどうかを判定することができる。たとえば、メッシュ・ネットワークを介して送信されるデータの一部が、メッシュ・ネットワークの様々なメンバー用である場合があり、他のデータが、アクセス・ゲートウェイ用である場合がある。モバイル・デバイスは、所期の宛先に基づいてこの判定を実行することができる（たとえば、データがアクセス・ゲートウェイ用である場合には、データはモバイル・デバイス用ではなく、データがモバイル・デバイス用である場合には、データはモバイル・デバイス用であり、かつ／またはデータがメッシュ・ネットワークの全メンバー用である場合には、データはモバイル・デバイス用である）。それに加えてまたはその代わりに、モバイル・デバイスは、データの解析に基づいてこの判定を実行することができる。たとえば、解析は、データのタイプを識別することができる（たとえば、電子メール同期化メッセージまたはメール同期化プロセスに関連するなんらかの他のタイプとしてタイプを識別する）。タイプの識別に基づいて、モバイル・デバイスは、データがそのデバイス用であるかどうかを判定することができる（たとえば、タイプが電子メール同期化メッセージである場合には、データはモバイル・デバイス用である可能性があり、タイプが企業リソースにアクセスする要求である場合には、データはモバイル・デバイス用ではない可能性があるなど）。データがモバイル・デバイス用であると判定する時に、この方法はステップ1125に進むことができる。モバイル・デバイスが、データがモバイル・デバイス用ではないと判定する場合には、この方法はステップ1127に進むことができる。

【0156】

ステップ1125では、モバイル・デバイスが、モバイル・デバイスのマネージド・アプリケーションにデータを供給することができる。たとえば、電子メール同期化メッセージが、モバイル・デバイスのマネージド・メール・アプリケーションに供給され得る。ウェブ・ブラウジング・メッセージが、モバイル・デバイスのマネージド・ブラウザ・アプリケーションに供給され得る。一般に、モバイル・デバイスは、モバイル・デバイスにインストールされた任意のマネージド・アプリケーションにデータを供給できる可能性がある。したがって、データは、そのタイプのデータを処理する任意のアプリケーションに供給され得る。

【0157】

ステップ1127では、モバイル・デバイスが、メッシュ・ネットワークを介してデータをルーティングし続けるべきかどうかを判定することができる。たとえば、メッシュ・ネットワークを介して送信されるデータの一部が、メッシュ・ネットワークの様々なメンバー用である場合があり、他のデータが、アクセス・ゲートウェイ用である場合がある。モバイル・デバイスは、所期の宛先に基づいてこの判定を実行することができる（たとえば、データがアクセス・ゲートウェイ用である場合には、データをルーティングし続け、データがモバイル・デバイスのみのためのものである場合には、データをルーティングし続けず、かつ／またはデータがメッシュ・ネットワークの全メンバー用である場合には、データをルーティングし続ける）。それに加えてまたはその代わりに、モバイル・デバイスは、データの解析に基づいてこの判定を実行することができる。たとえば、解析は、データのタイプを識別することができる（たとえば、電子メール同期化メッセージまたはメール同期化プロセスに関連するなんらかの他のタイプとしてタイプを識別する）。タイプの識

別に基づいて、モバイル・デバイスは、データをルーティングし続けるべきかどうかを判定することができる（たとえば、タイプが電子メール同期化メッセージである場合には、データをルーティングし続け、タイプが企業リソースにアクセスする要求である場合には、データをルーティングし続け、タイプがチャット・メッセージである場合には、データをルーティングし続けないなど）。

【0158】

さらに、モバイル・デバイスは、メッシュ・ネットワーク内でモバイル・デバイスのために確立されたピアツーピア接続および／またはデータがその上で受信されたピアツーピア接続の個数に基づいてこの判定を実行することができる。たとえば、図9の例示的な配置を使用すると、モバイル・デバイス902-Bが、ピアツーピア接続903を介してデータを受信した場合に、モバイル・デバイス902-Bは、ピアツーピア接続904が確立されていることに基づいてルーティングを続けると判定することができる。さらに、モバイル・デバイス902-Bは、データの別のコピーが以前にピアツーピア接続904を介して受信されたかどうかを判定することができ、データの別のコピーが以前にピアツーピア接続904を介して受信された場合には、モバイル・デバイスは、データをルーティングし続けないと判定することができる。別の例として、図7の例示的な配置を使用すると、モバイル・デバイス702-Aが、ピアツーピア接続703を介してデータを受信した場合に、モバイル・デバイス702-Aは、他のピアツーピア接続が存在しないと判定することができ、したがって、データをルーティングし続けないと判定することができる。

【0159】

メッシュ・ネットワークを介してデータをルーティングし続けると判定する時に、この方法はステップ1129に進むことができる。モバイル・デバイスが、メッシュ・ネットワークを介してデータをルーティングし続けないと判定する場合に、この方法は終了することができる。

【0160】

ステップ1129では、モバイル・デバイスが、メッシュ・ネットワーク内の1つまたは複数の次のホップにデータをルーティングすることができる。このステップは、図11Aのステップ1103～1109によって表される反復プロセスと同様に実行され得る。たとえば、メッシュ・ネットワーク内の1つまたは複数の次のホップへのデータのルーティングは、モバイル・デバイスに、各次のホップに対応する1つまたは複数のピアツーピア通信を使用してメッシュ・ネットワーク上の1つまたは複数の次のホップにデータを送信させるために、ステップ1103～1109によって表される反復プロセスを実行することによって実行され得る。特定の例として、図9の例示的な配置を使用すると、モバイル・デバイス902-Bが、ピアツーピア接続903を介してデータを受信した場合に、モバイル・デバイス902-Bは、ピアツーピア接続906を介してデータを送信することによって、モバイル・デバイス902-Dにデータをルーティングするために反復プロセスを実行することができる。

【0161】

さらに、いくつかの配置では、モバイル・デバイス902-Bは、モバイル・デバイス902-Dに暗号化された形でデータをルーティングするために反復プロセスを実行することができる（たとえば、図11Aのステップ1105に関連して議論したように）。さらに、いくつかの配置で、暗号化された形は、メッシュ・ネットワーク内のピアツーピア接続のそれぞれについて異なるものとすることができる（たとえば、ピアツーピア接続903は、ピアツーピア接続905とは異なる暗号化鍵／暗号化解除鍵を使用する）。したがって、これらの配置のうちの1つまたは複数では、データは、まず、そのデータがその上で受信されたピアツーピア接続に基づいて暗号化解除され得（たとえば、図11Bのステップ1122に関連して議論したように）、そのデータがその上でメッシュ・ネットワーク内の次のホップに送信されるピアツーピア接続に基づいて再暗号化され得（たとえば、図11Aのステップ1105に関連して議論したように）。しかし、いくつかの変形

形態では、メッシュ・ネットワークは、ピアツーピア接続ごとに同一の暗号化方式を使用することができる。したがって、これらの変形形態のうちの1つまたは複数では、データがピアツーピア接続を介して受信された場合に、データまたはその一部は、暗号化解除され、再暗号化される必要がない可能性がある（たとえば、図11Bのステップ1122に関連して議論した暗号化解除が、実行されなくてもよく、図11Aのステップ1105に関連して議論した暗号化が、実行されなくてもよい）。

【0162】

図11Cは、モバイル・デバイスがピアツーピア接続を介して受信したデータを、仮想プライベート・ネットワーク接続を使用してアクセス・ゲートウェイに送信できる、例の方法を示す。いくつかの配置では、図11Cの例の方法は、確立された仮想プライベート・ネットワーク接続を有するデバイス（たとえば、モバイル・デバイス702-C、モバイル・デバイス902-C、および／またはモバイル・デバイス902-D）によって実行され得る。さらに、いくつかの配置で、図11Cの例の方法は、現在選択されている（たとえば、図10Aのステップ1011によって選択され、または図10Bの例の方法によって判定される変化を介して選択される）確立された仮想プライベート・ネットワーク接続を有するデバイスによって実行され得る。

10

【0163】

ステップ1141では、モバイル・デバイスが、メッシュ・ネットワークのピアツーピア接続を介してデータを受信することができる。このステップは、図11Bのステップ1121と同様に実行され得る。

20

【0164】

ステップ1142では、モバイル・デバイスが、ステップ1141で受信されたデータを処理することができる。このステップは、図11Bのステップ1122と同様に実行され得る。

【0165】

ステップ1143では、モバイル・デバイスが、ステップ1141で受信され、ステップ1142で処理されたデータが、モバイル・デバイス用であるかどうかを判定することができる。このステップは、図11Bのステップ1123と同様に実行され得る。

【0166】

ステップ1145では、モバイル・デバイスが、モバイル・デバイスのマネージド・アプリケーションにデータを供給することができる。このステップは、図11Bの1135と同様に実行され得る。

30

【0167】

ステップ1147では、モバイル・デバイスが、仮想プライベート・ネットワーク接続を介してデータを送信すべきかどうかを判定することができる。たとえば、メッシュ・ネットワークを介して送信されるデータの一部分が、メッシュ・ネットワークの様々なメンバーである場合があり、他のデータが、アクセス・ゲートウェイ用である場合がある。モバイル・デバイスは、所期の宛先に基づいてこの判定を実行することができる（たとえば、データがアクセス・ゲートウェイ用である場合には、仮想プライベート・ネットワーク接続を介してデータを送信し、データがモバイル・デバイスのみのためのものである場合には、仮想プライベート・ネットワーク接続を介してデータを送信せず、かつ／またはデータがメッシュ・ネットワークのメンバーのみのためのものである場合には、仮想プライベート・ネットワーク接続を介してデータを送信しない）。それに加えてまたはその代わりに、モバイル・デバイスは、データの解析に基づいてこの判定を実行することができる。たとえば、解析は、データのタイプを識別することができる（たとえば、電子メール同期化メッセージまたはメール同期化プロセスに関連するなんらかの他のタイプとしてタイプを識別する）。タイプの識別に基づいて、モバイル・デバイスは、仮想プライベート・ネットワーク接続を介してデータを送信すべきかどうかを判定することができる（たとえば、タイプが電子メール同期化メッセージである場合には、仮想プライベート・ネットワーク接続を介してデータを送信せず、タイプが企業リソースにアクセスする要求である場合に

40

50

は、仮想プライベート・ネットワーク接続を介してデータを送信し、タイプがチャット・メッセージである場合には、仮想プライベート・ネットワーク接続を介してデータを送信しないなど）。

【0168】

仮想プライベート・ネットワーク接続を介してデータを送信すべきであると判定する時に、この方法はステップ1149に進むことができる。モバイル・デバイスが、仮想プライベート・ネットワーク接続を介してデータを送信すべきではないと判定する場合には、この方法は終了することができる。

【0169】

ステップ1149では、モバイル・デバイスが、仮想プライベート・ネットワーク接続を介してアクセス・ゲートウェイにデータを送信することができる。たとえば、モバイル・デバイスは、仮想プライベート・ネットワーク接続に関連するプロトコルに従うようにデータを処理することができ、かつ／または仮想プライベート・ネットワーク接続によって要求される通りにデータを暗号化することができる。処理された後に、モバイル・デバイスは、データをアクセス・ゲートウェイに送信することができる。受信時に、アクセス・ゲートウェイは、適宜データを処理することができる（たとえば、企業リソース／サービスへのアクセスを可能にするなど）。

【0170】

さらに、いくつかの実施形態では、図11Cの例の方法を終了する前に、モバイル・デバイスは、メッシュ・ネットワークのメンバにデータをルーティングし続けるべきかどうかを判定することができる。この判定は、図11Bのステップ1127と同様に実行され得る。データをルーティングし続けると判定する時に、モバイル・デバイスは、しかるべくデータをルーティングするために進行することができる（たとえば、図11Bのステップ1129と同様にルーティングすることによって）。モバイル・デバイスがデータをルーティングし続けるべきではないと判定する場合には、この方法は終了することができる。代替案では、モバイル・デバイスは、ピアツーピア接続を介してデータを受信する時に、図11Bおよび図11Cの両方の例の方法を実行することができる、各例の方法は、それ自体のスレッド内で実行される。

【0171】

図11Dは、モバイル・デバイスが、それが仮想プライベート・ネットワーク接続を介して受信するデータをメッシュ・ネットワークの次のホップにルーティングできる、例の方法を示す。いくつかの配置では、図11Dの例の方法は、確立された仮想プライベート・ネットワーク接続を有するデバイス（たとえば、モバイル・デバイス702-C、モバイル・デバイス902-C、および／またはモバイル・デバイス902-D）によって実行され得る。さらに、いくつかの配置で、図11Dの例の方法は、現在選択されている（たとえば、図10Aのステップ1011によって選択され、または図10Bの例の方法によって判定される変化を介して選択される）確立された仮想プライベート・ネットワーク接続を有するデバイスによって実行され得る。

【0172】

ステップ1161では、モバイル・デバイスが、仮想プライベート・ネットワーク接続を介してアクセス・ゲートウェイからデータを受信することができる。いくつかの例で、このデータは、仮想プライベート・ネットワーク接続を介するアクセス・ゲートウェイへの以前のデータ送信に応答するものとすることができる。他の例では、このデータは、アクセス・ゲートウェイによってメッシュ・ネットワークの1つまたは複数のメンバにブッシュされつつあるデータとすることができる。データの受信時に、モバイル・デバイスは、図11Dの残りのステップに進む前にデータを処理することができる（たとえば、仮想プライベート・ネットワークデータ通信からデータを抽出する、データを暗号化解除するなど）。

【0173】

ステップ1163では、モバイル・デバイスは、データがモバイル・デバイス用である

10

20

30

40

50

かどうかを判定することができる。このステップは、図11Bのステップ1123と同様に実行され得る。

【0174】

ステップ1165では、モバイル・デバイスが、モバイル・デバイスのマネージド・アプリケーションにデータを供給することができる。このステップは、図11Bの1135と同様に実行され得る。

【0175】

ステップ1167では、モバイル・デバイスが、メッシュ・ネットワークを介してデータをルーティングすべきかどうかを判定することができる。たとえば、仮想プライベート・ネットワーク接続を介して受信されるデータの一部が、メッシュ・ネットワークの様々なメンバ用である場合があり、他のデータが、モバイル・デバイスのみのためのものである場合がある。モバイル・デバイスは、所期の宛先に基づいてこの判定を実行することができる（たとえば、データが、モバイル・デバイスのみのためのものである場合には、メッシュ・ネットワークを介してデータをルーティングせず、データが、メッシュ・ネットワークのメンバ用である場合には、メッシュ・ネットワークを介してデータをルーティングし、データが、メッシュ・ネットワークの全メンバ用である場合には、メッシュ・ネットワークを介してデータをルーティングする）。それに加えてまたはその代わりに、モバイル・デバイスは、データの解析に基づいてこの判定を実行することができる。たとえば、解析は、データのタイプを識別することができる（たとえば、電子メール・メッセージまたは電子メール・サービスに関連するなんらかの他のタイプとしてタイプを識別する）。タイプの識別に基づいて、モバイル・デバイスは、メッシュ・ネットワークを介してデータをルーティングすべきかどうかを判定することができる（たとえば、タイプが電子メール・メッセージである場合には、メッシュ・ネットワークを介してデータをルーティングするなど）。

【0176】

メッシュ・ネットワークを介してデータをルーティングすると判定する時に、この方法はステップ1169に進むことができる。モバイル・デバイスが、メッシュ・ネットワークを介してデータをルーティングしないと判定する場合には、この方法は終了することができる。

【0177】

ステップ1169では、モバイル・デバイスが、メッシュ・ネットワーク内の1つまたは複数の次のホップにデータをルーティングすることができる。このステップは、図11Bのステップ1129と同様に実行され得る。特定の例として、図9の例示的な配置を使用すると、モバイル・デバイス902-Dが、仮想プライベート・ネットワーク接続913を介してデータを受信した場合に、モバイル・デバイス902-Dは、それぞれピアツーピア接続906および905を介してデータを送信することによって、モバイル・デバイス902-Bおよび902-Cにデータをルーティングするために反復プロセスを実行することができる。

【0178】

図12は、メッシュ・ネットワークの確立を示す例のフローと、本明細書で説明される態様に従う企業モビリティ管理システムに関連する様々な機能の実行に関連するメッシュ・ネットワークの使用とを示す図である。具体的には、例のフローは、図7～図11Dを含む本開示全体で説明される配置および例の方法に従って実行され得る複数の機能を示す。

【0179】

図12に示されているように、3つのモバイル・デバイスすなわちモバイル・デバイス1201、1203、および1205が、お互いからしきい距離以内にある。3つのモバイル・デバイスのそれぞれは、同一のユーザに関連付けられ得る。図12に示されたデバイスの配置は、図7および図9の例の配置に類似するが、単純さのために、様々なピアツーピア接続および介在するネットワークは、図12から省略されている。図12の例で説

明される様々なフローを介して、モバイル・デバイス1201、1203、および1205は、メッシュ・ネットワークを確立し、メッシュ・ネットワークのメンバと通信し、アクセス・ゲートウェイ1207とメッシュ・ネットワークのメンバのうちの1つとの間で確立された仮想プライベート・ネットワーク接続を介してアクセス・ゲートウェイ120と通信することができる可能性がある。図12に示された様々なフローは、様々なデバイスの間の1つまたは複数の通信を含むことができる、図8、図10A、図10B、および図11A～図11Dで議論された例の方法のうちの1つまたは複数の実行をさらに含むことができる。

【0180】

フロー1231で開始して、モバイル・デバイス1205およびアクセス・ゲートウェイ1207は、お互いの間で仮想プライベート・ネットワーク接続を確立することができる。仮想プライベート・ネットワーク接続の確立は、セキュリティ証明書およびモバイル・デバイス1205を認証するためにアクセス・ゲートウェイによって要求される他のユーザ情報の送信を含むことができる。アクセス・ゲートウェイは、SSOのために構成された有効な認証トークンをモバイル・デバイス1205にさらに供給することができる。フロー1231に関連して示された矢印は、仮想プライベート・ネットワーク接続の確立に関連してモバイル・デバイス1205とアクセス・ゲートウェイ1207との間で交換され得る様々な送信を表すためのものである。

【0181】

フロー1233では、モバイル・デバイス1201、1203、および1205は、お互いの間でメッシュ・ネットワークを確立することができる。メッシュ・ネットワークの確立は、各デバイスが図8または図10A（あるいはそのなんらかの変形形態）の例の方法のうちの1つを実行することを含むことができる。たとえば、ユーザは、デバイス1201上でメッシュ・ネットワークを確立する試みを開始することができる。デバイス1205は、デバイス1201および1203でユーザが入力したまたは確認しなければならないPINコード（たとえば、図8のステップ801）を表示するように構成され得る。PINコードは、デバイス1201および1203をメッシュ・ネットワークのメンバとして認可することに関連して使用され得る。フロー1233に関連して示された矢印は、モバイル・デバイスの間で送信されるはずの（たとえば、ピアツーピア通信および／またはピアツーピア接続を使用して）様々な通信を表すためのものである。

【0182】

フロー1235では、モバイル・デバイス1205は、メッシュ・ネットワーク内の他のメンバのためにSSOを使用可能にするために進行することができる。いくつかの配置では、これは、SSOのために構成された有効な認証トークンをメッシュ・ネットワークを介してモバイル・デバイス1201および1203にルーティングすることを含むことができる。たとえば、モバイル・デバイス1205は、SSOのために構成された有効な認証トークンが1つまたは複数のピアツーピア接続を介して送信されるようにするために、図11Aの例の方法を実行することができる。モバイル・デバイス1203は、SSOのために構成された有効な認証トークンを受信し、SSOのために構成された有効な認証トークンを後の使用のために処理し、SSOのために構成された有効な認証トークンをメッシュ・ネットワークを介して次のホップすなわちモバイル・デバイス1201にルーティングするために、図11Bの例の方法を実行することができる。モバイル・デバイス1201は、SSOのために構成された有効な認証トークンを受信し、後の使用のためにこれを処理するために、図11Bの例の方法を実行することができる。フロー1235に関連して示された矢印は、モバイル・デバイス1201と1203との両方がSSOのために構成された有効な認証トークンを受信するようにするために、メッシュ・ネットワークを介して送信されるはずの様々な通信を表すためのものである。

【0183】

いくつかの配置では、メッシュ・ネットワーク内の他のメンバのためにSSOを使用可能にするフロー1235に基づいて、モバイル・デバイス1201および1203上のセ

10

20

30

40

50

セキュア・コンテナは、モバイル・デバイス1205から送信された認証トークンに基づいて、使用のためにアンロックされ得る。たとえば、モバイル・デバイス1201および1203は、通常はパスワード、PINコード、または他のセキュリティ証明書によってアンロックされるセキュア・コンテナを含むことができる。ユーザがパスワード、PINコードなどを入力することを要求するのではなく、モバイル・デバイス1205から送信された認証トークンが、モバイル・デバイス1201および1203によって、セキュア・コンテナをアンロックするのに使用され得る。この形で、モバイル・デバイス1201および1203は、それらのそれぞれのセキュア・コンテナに対してSSOと共に使用可能にされ得る。モバイル・デバイス1205から送信された認証トークンは、たとえばマネージド・アプリケーションのためにSSOを使用可能にすることを含む、企業管理フレームワークの様々な他の構成要素のSSOを使用可能にするのに使用され得る。

10

【0184】

フロー1237では、モバイル・デバイス1203は、アクセス・ゲートウェイ1207によって制御され、かつ／または管理される企業リソース1209にアクセスすることができる。いくつかの配置では、これは、モバイル・デバイス1205が仮想プライベート・ネットワーク接続を介してデータを送信できるようにするために、企業リソース1209にアクセスする要求を示すデータをルーティングすることを含むことができる。たとえば、モバイル・デバイス1203は、企業リソース1209にアクセスする要求を示すデータがピアツーピア接続を介して次のホップすなわちモバイル・デバイス1205に送信されるようにするために、図11Aの例の方法を実行することができる。いくつかの配置で、データは、SSOのために構成された有効な認証トークンを含むことができる（たとえば、モバイル・デバイス1203が、企業リソース1209にアクセスするためにアクセス・ゲートウェイ1207と共にシームレス認証を実行できるようにするために）。モバイル・デバイス1205は、データがピアツーピア接続を介して受信され、仮想プライベート・ネットワーク接続を介してアクセス・ゲートウェイ1207に送信されるようにするために、図11Cの例の方法を実行することができる。受信時に、アクセス・ゲートウェイ1207は、SSOのために構成された有効な認証トークンに基づいて、要求を認証し、企業リソース1209への要求されたアクセスを実行することができる。要求されたアクセスは、応答データ（たとえば、モバイル・デバイス1205によって要求されている特定のファイル）を生成することができ、応答データが、仮想プライベート・ネットワーク接続を介してモバイル・デバイス1205に送信され得る。モバイル・デバイス1205は、応答データが仮想プライベート・ネットワーク接続を介して受信され、メッシュ・ネットワークを介して次のホップすなわちモバイル・デバイス1203にルーティングされるようにするために、図11Dの例の方法を実行することができる。モバイル・デバイス1203は、応答データが受信され、しかるべく処理されるようにするために、図11Bの例の方法を実行することができる。フロー1237に関連して示された矢印は、モバイル・デバイス1203が企業リソース1209に成功裡にアクセスできるようにするために、メッシュ・ネットワークを介し、仮想プライベート・ネットワーク接続を介し、アクセス・ゲートウェイ1207と企業リソース1209との間で送信される様々な通信を表すためのものである。

20

30

40

【0185】

フロー1239では、モバイル・デバイス1201は、アクセス・ゲートウェイ1207によって制御され、かつ／または管理される企業サービス1211にアクセスすることができる。いくつかの配置で、これは、モバイル・デバイス1205が仮想プライベート・ネットワーク接続を介してデータを送信できるようにするために、企業サービス1211にアクセスする要求を示すデータをメッシュ・ネットワークを介してルーティングすることを含むことができる。たとえば、モバイル・デバイス1201は、企業サービス1211にアクセスする要求を示すデータがピアツーピア接続を介して次のホップすなわちモバイル・デバイス1203に送信されるようにするために、図11Aの例の方法を実行することができる。いくつかの配置で、データは、SSOのために構成された有効な認証ト

50

ークンを含むことができる（たとえば、モバイル・デバイス1201が、企業サービス1211にアクセスするためにアクセス・ゲートウェイと共にシームレス認証を実行できるようにするために）。モバイル・デバイス1203は、データが、ピアツーピア接続を介して受信され、メッシュ・ネットワークを介して次のホップすなわちモバイル・デバイス1205に送信されるようにするために、図11Bの例の方法を実行することができる。モバイル・デバイス1205は、データが、ピアツーピア接続を介して受信され、仮想プライベート・ネットワーク接続を介してアクセス・ゲートウェイ1207に送信されるようにするために、図11Cの例の方法を実行することができる。受信時に、アクセス・ゲートウェイ1207は、SSOのために構成された有効な認証トークンに基づいて、要求を認証し、企業サービス1211への要求されたアクセスを実行することができる。要求されたアクセスは、応答データ（たとえば、ファイル共有サービスによって共有されるファイルのリスティング）を生成することができ、応答データは、仮想プライベート・ネットワーク接続を介してモバイル・デバイス1205に送信され得る。モバイル・デバイス1205は、応答データが仮想プライベート・ネットワーク接続を介して受信され、メッシュ・ネットワークを介して次のホップすなわちモバイル・デバイス1203にルーティングされるようにするために、図11Dの例の方法を実行することができる。モバイル・デバイス1203は、応答データがピアツーピア接続を介して受信され、メッシュ・ネットワークを介して次のホップすなわちモバイル・デバイス1201にルーティングされるようにするために、図11Bの例の方法を実行することができる。モバイル・デバイス1201は、応答データが受信され、しかるべく処理されるようにするために、図11Bの例の方法を実行することができる。フロー1239に関連して示された矢印は、モバイル・デバイス1201が企業サービス1211に成功裡にアクセスできるようにするために、メッシュ・ネットワークを介し、仮想プライベート・ネットワーク接続を介し、アクセス・ゲートウェイ1207と企業サービス1211との間で送信されるはずの様々な通信を表すためのものである。

【0186】

フロー1241では、モバイル・デバイス1203は、そのスクリーンをモバイル・デバイス1201と共有することができる。いくつかの配置では、これは、モバイル・デバイス1203のスクリーンのグラフィカル・データを準備することと、モバイル・デバイス1201がそのグラフィカル・データを表示できるようにするためにメッシュ・ネットワークを介してそのグラフィカル・データをルーティングすることとを含むことができる。たとえば、モバイル・デバイス1203は、グラフィカル・データを準備し、そのグラフィカル・データを次のホップすなわちモバイル・デバイス1201にルーティングするために、図11Aの例の方法を実行することができる。モバイル・デバイス1201は、グラフィカル・データを受信し、しかるべく処理するために、図11Bの例の方法を実行することができる。いくつかの配置では、モバイル・デバイス1201のユーザは、グラフィカル・データと対話できる可能性がある（たとえば、共有されるスクリーンを介して示されるテキスト文書の諸部分を強調表示する、文書にコピー・アクションを実行する、文書に貼り付けアクションを実行するなど）。そのような配置では、モバイル・デバイス1201は、1つまたは複数のユーザ対話を示すデータを準備し、メッシュ・ネットワークを介してそのデータを次のホップすなわちモバイル・デバイス1203にルーティングするために、図11Aの例の方法を実行することができる。モバイル・デバイス1203は、1つまたは複数のユーザ対話を示すデータ受信し、これをしかるべく処理する（たとえば、1つまたは複数のユーザ対話に基づいてスクリーンを操作する）ために、図11Bの例の方法を実行することができる。フロー1241に関連して示された矢印は、モバイル・デバイス1201が企業サービス1211に成功裡にアクセスできるようにするために、メッシュ・ネットワークを介し、仮想プライベート・ネットワーク接続を介し、アクセス・ゲートウェイ1207と企業サービス1211との間で送信されるはずの様々な通信を表すためのものである。

【0187】

フロー1243では、アクセス・ゲートウェイ1207が、メッシュ・ネットワークの1つまたは複数のメンバにポリシ更新をプッシュすることができる。モバイル・デバイス1201、1203、および1205のそれぞれは、それぞれのモバイル・デバイスのアプリケーション管理フレームワークによって実施されるポリシを記憶することができる。図12に示されているように、ポリシ更新は、メッシュ・ネットワークのすべてのメンバにプッシュされる。いくつかの配置では、ポリシ更新のプッシュは、アクセス・ゲートウェイ1207が、更新されたポリシを判定することと、更新されたポリシを仮想プライベート・ネットワーク接続を介してモバイル・デバイス1205に送信することを含むことができる。モバイル・デバイス1205は、更新されたポリシが仮想プライベート・ネットワーク接続を介して受信され、モバイル・デバイス1205によって記憶されるポリシを更新するために処理され、メッシュ・ネットワークを介して次のホップすなわちモバイル・デバイス1203にルーティングされるようにするために、図11Dの例の方法を実行することができる。モバイル・デバイス1203は、更新されたポリシがピアツーピア接続を介して受信され、モバイル・デバイス1203によって記憶されるポリシを更新するために処理され、次のホップすなわちモバイル・デバイス1201にルーティングされるようにするために、図11Bの例の方法を実行することができる。モバイル・デバイス1201は、更新されたポリシが受信され、モバイル・デバイス1201によって記憶されるポリシを更新するために処理されるようにするために、図11Bの例の方法を実行することができる。フロー1243に関連して示された矢印は、アクセス・ゲートウェイ1207がメッシュ・ネットワークの各メンバに更新されたポリシを成功裡にプッシュできるようにするために、メッシュ・ネットワークを介し、仮想プライベート・ネットワーク接続を介して送信されるはずの様々な通信を表すためのものである。

【0188】

図12に関連して説明された上のフローは、本明細書で説明される配置またはその変形形態を使用して実行され得る機能のタイプの少数の例のみを提供する。たとえば、SSOの使用可能化および／またはデバイスの間でのスクリーンの共有に加えて、モバイル・デバイス1201、1203、および1205は、メッシュ・ネットワークのメンバの間でチャット・メッセージを送信し、メッシュ・ネットワークのメンバにおよびこれらのメンバからファイルをコピーし、メッシュ・ネットワークのメンバの間でファイルまたは他のデータを共有するなどのために、メッシュ・ネットワークを介して通信することができる。別の例として、企業リソース1209または12011へのアクセスに加えて、モバイル・デバイス1201、1203、および1205は、マネージド・ブラウジング・アプリケーションに関連してインターネットにアクセスするために、メッシュ・ネットワークを介してアクセス・ゲートウェイ1207と通信することができる。

【0189】

本主題が、構造的特徴および／または方法論的行為に固有の言葉で説明されたが、添付の特許請求の範囲で定義される本主題が、必ずしも上で説明された特定の特徴または行為に限定されないことを理解されたい。そうではなく、上で説明された特定の特徴および行為は、以下の特許請求の範囲の例の実施態様として説明される。

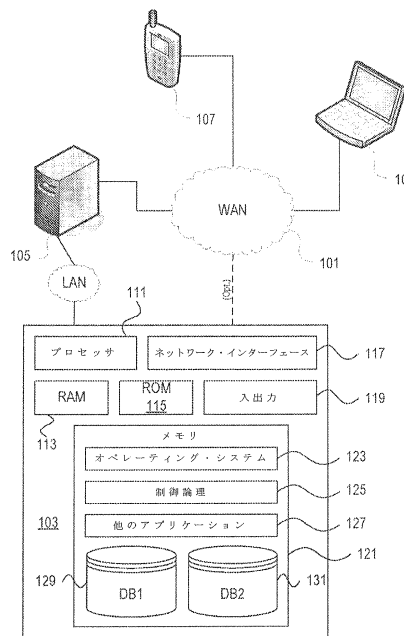
【0190】

関連出願の相互参照

本願は、その全体が参照によってあらゆる目的について本明細書に組み込まれている、2017年3月6日に出願した米国特許非仮出願第15/450654号、名称「VIRTUAL PRIVATE NETWORKING BASED ON PEER-TO-PEER COMMUNICATION」の優先権を主張するものである。

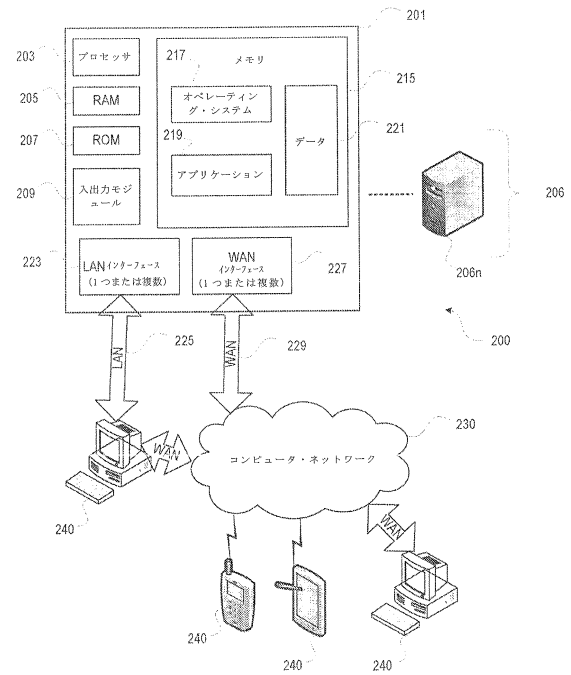
【図 1】

【図 1】



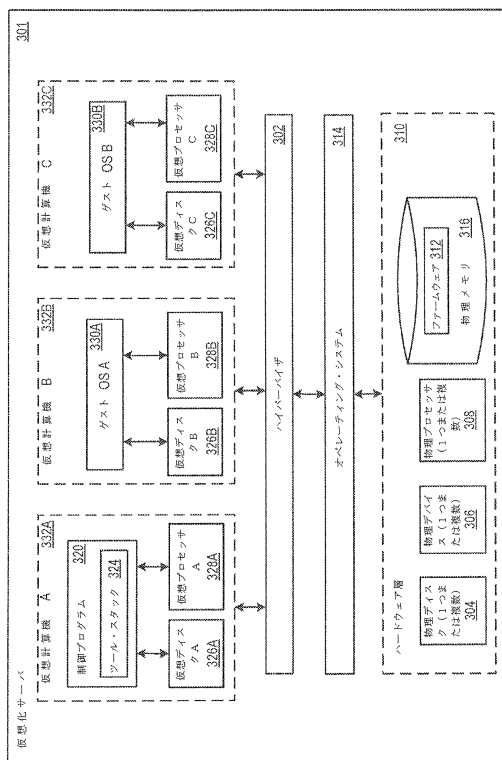
【図 2】

【図 2】



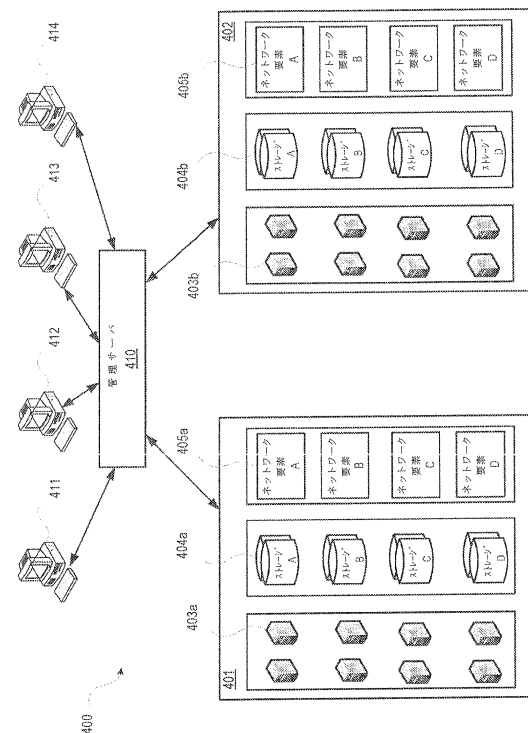
【図 3】

【図 3】



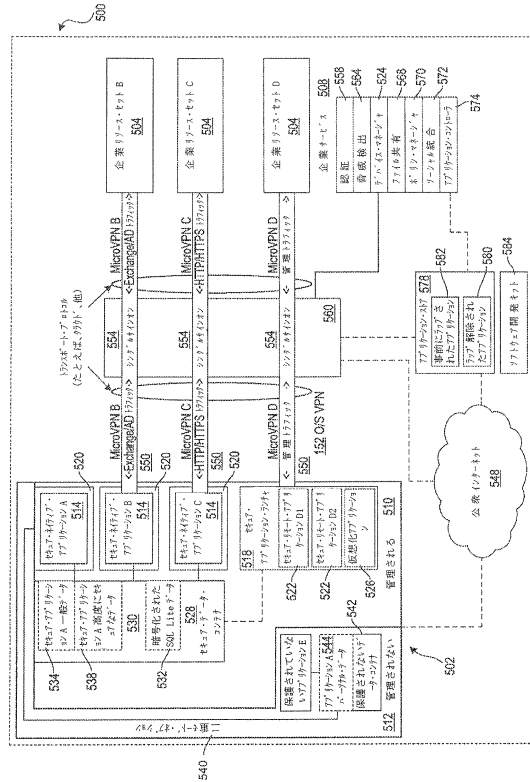
【図 4】

【図 4】



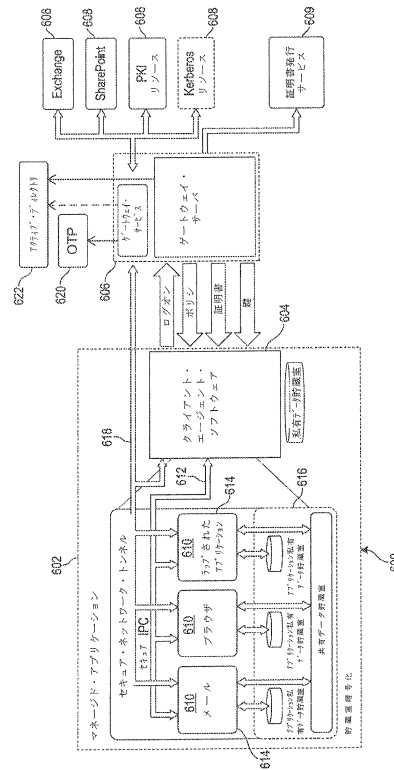
【図 5】

【図 5】



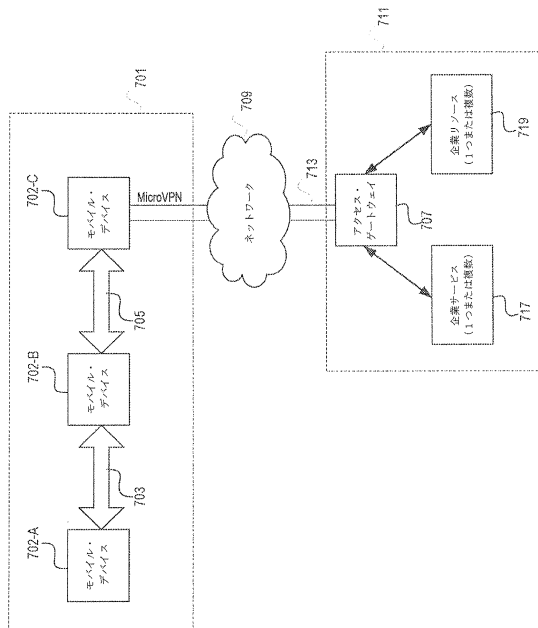
【図 6】

【図 6】



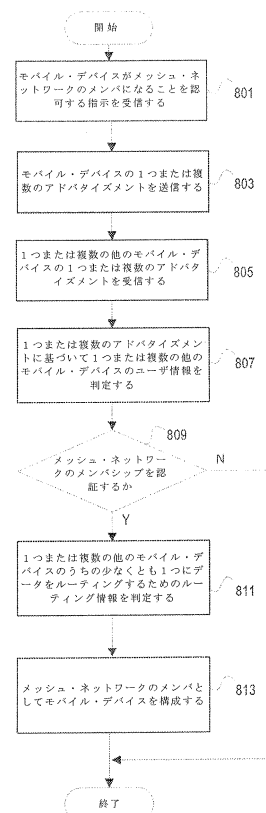
【図 7】

【図 7】



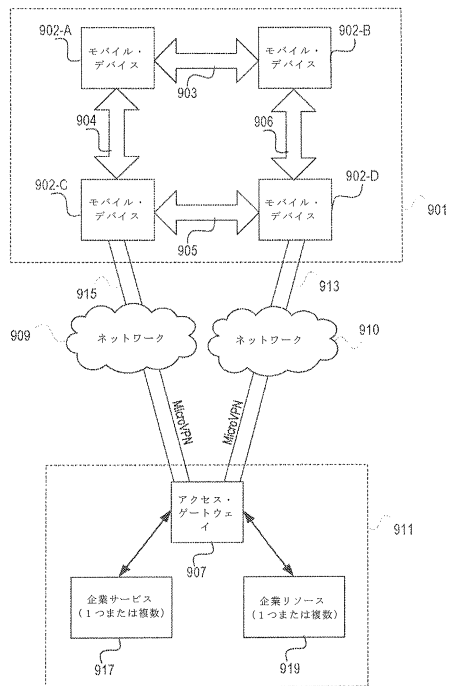
【図 8】

【図 8】



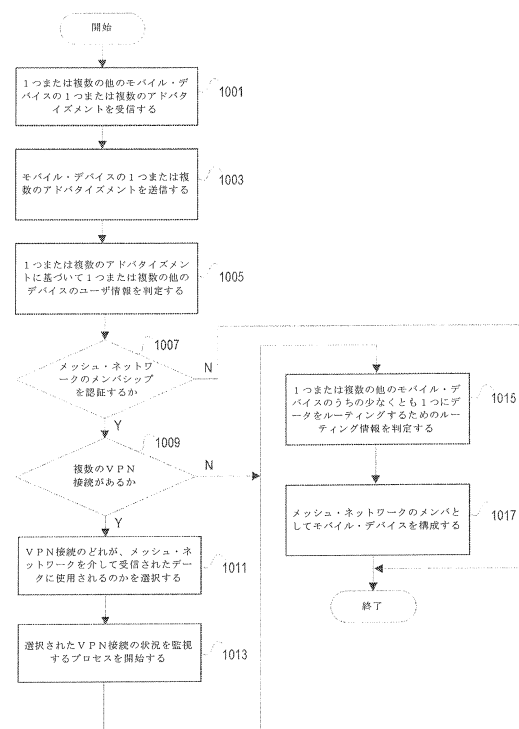
【図 9】

【図 9】



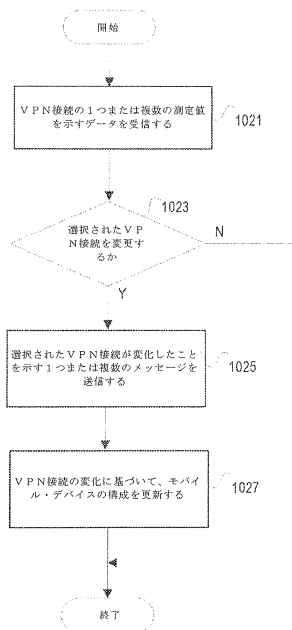
【図 10 A】

【図 10 A】



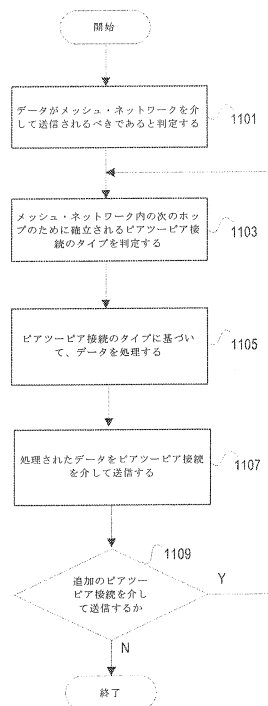
【図 10 B】

【図 10 B】



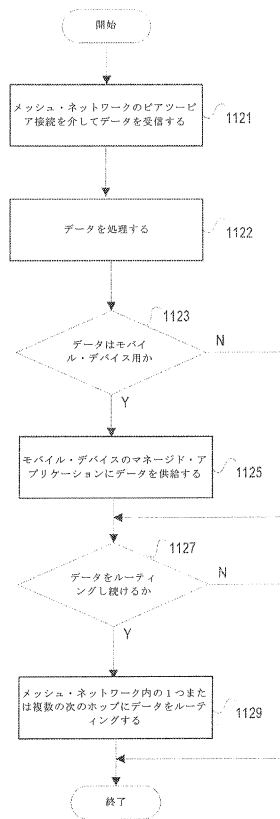
【図 11 A】

【図 11 A】



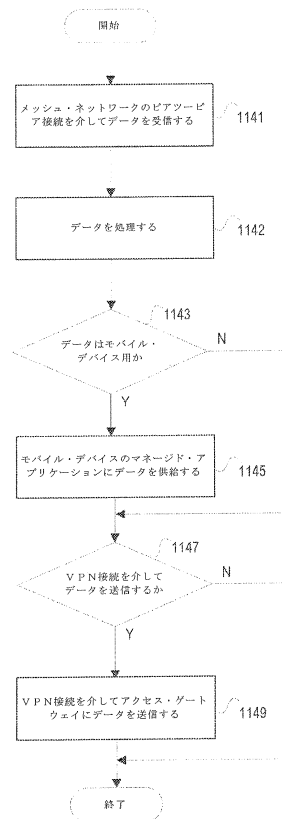
【図 1 1 B】

【図 1 1 B】



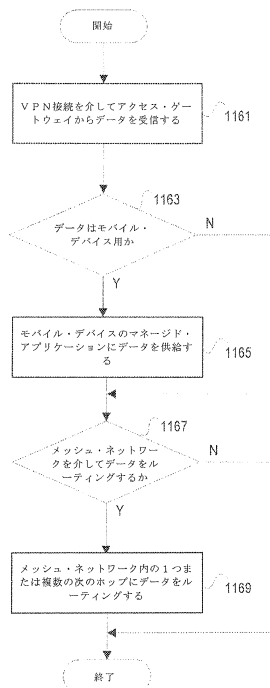
【図 1 1 C】

【図 1 1 C】



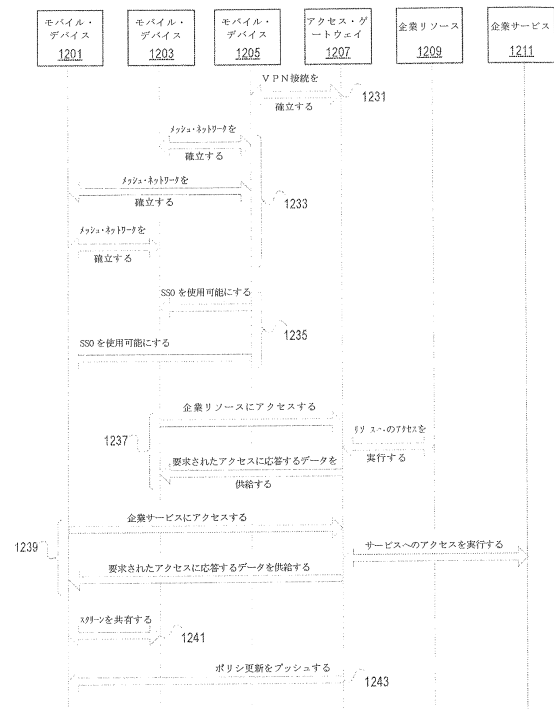
【図 1 1 D】

【図 1 1 D】



【図 1 2】

【図 1 2】



フロントページの続き

(51)Int.Cl. F I
H 0 4 L 12/70 (2013.01) H 0 4 L 12/70 D

(72)発明者 ケネル, グラント
アメリカ合衆国, フロリダ州 33309, フォート ローダーデール, ウェスト サイプレス
クリーク ロード 851, サイトリックス システムズ, インコーポレイテッド内

(72)発明者 シン, ジャスプリート
アメリカ合衆国, フロリダ州 33309, フォート ローダーデール, ウェスト サイプレス
クリーク ロード 851, サイトリックス システムズ, インコーポレイテッド内

審査官 中野 修平

(56)参考文献 特表2016-517647 (JP, A)
特表2016-526223 (JP, A)
特表2011-524657 (JP, A)
特開2005-184835 (JP, A)

(58)調査した分野(Int.Cl., DB名)
H 0 4 B 7/24- 7/26
H 0 4 L 12/70
H 0 4 W 4/00-99/00
3 G P P T S G R A N W G 1-4
S A W G 1-4
C T W G 1、4